GlobalResearch
Center for Research on Globalization

“Virus Mitigation”, “Track and Trace”: The CDC Surveilled for Covid Lockdown Compliance

By Jeffrey A. Tucker
Global Research, May 08, 2022
Brownstone Institute 4 May 2022

Region: USA
Theme: Intelligence, Law and Justice

***

A missing piece of the great lockdown plot was enforcement. How precisely were authorities going to know the whereabouts of hundreds of millions of people without a veritable army of snoops?

Yes, there were some arrests and media reports and some private drones flying here and there to snap pictures of house parties to send to local papers for publication. Public health authorities were flooded with calls from rats coast to coast.

But in general, the plan to muscle the entire population in the name of virus mitigation had vast holes.

For example, for many months, there were regulations in place that forced people to quarantine (yes, even if you were perfectly well) when crossing state lines. Compliance was impossible for anyone who lived in one state and worked in another. But how was this to be enforced? And how precisely were authorities to know for certain whether you found a side entrance to a church and dared to show up with a few others to pray?

A clue came pretty early on in lockdowns. When you would drive from one border to another, your phone would light up with a warning that you had to quarantine for two weeks before you went back, and then one would receive another note coming back. Of course this was impossible but it became darn scary there for a while. Who precisely was monitoring this?

Our phones also installed for us, even if we didn’t want it, track-and-trace software that claimed to alert you if you came near a covid-positive person as if this virus was Ebola and infected people were milling around everywhere. I have heard no reports on how this software worked or if it did at all.

Still it’s on my phone now – labeled “exposure notifications” – but obviously shut off. There

is no way to remove that application so far as I can tell.

Wikipedia explains:

> Devices record received messages, retaining them locally for 14 days. If a user tests positive for infection, the last 14 days of their daily encryption keys can be uploaded to a central server, where it is then broadcast to all devices on the network. The method through which daily encryption keys are transmitted to the central server and broadcast is defined by individual app developers. The Google-developed reference implementation calls for a health official to request a one-time verification code (VC) from a verification server, which the user enters into the encounter logging app. This causes the app to obtain a cryptographically signed certificate, which is used to authorize the submission of keys to the central reporting server

So, basically a digital leper bell. Just what everyone wants.

I had friends who flew into airports and were greeted by National Guard troops demanding information on where people were staying plus a cell phone number so that authorities could check to make sure that you were staying put and not going places. Government set up robocalls with scary voices – "This is the sheriff's office" – that would ring up visitors and scare the heck out of them.

Yes, you could lie, but what if you were caught? Were there criminal penalties? And what was the likelihood that you would get caught? No one knew for sure. Even the legal basis for all of this was extremely sketchy: it was all based on administrative dictate imposed under the cover of emergency.

As it turns out, the CDC later used your tax dollars to scarf up location data from shady sources during the depth of lockdowns to find out whether and to what extent people were complying with unconstitutional lockdowns, curfews, and capacity restrictions. We only know this thanks to a FOIA request from Motherboard, which revealed everyone's worst-possible fear. According to Vice,

> The Centers for Disease Control and Prevention (CDC) bought access to location data harvested from tens of millions of phones in the United States to perform analysis of compliance with curfews, track patterns of people visiting K-12 schools, and specifically monitor the effectiveness of policy in the Navajo Nation, according to CDC documents obtained by Motherboard. The documents also show that although the CDC used COVID-19 as a reason to buy access to the data more quickly, it intended to use it for more general CDC purposes.

In documents, the CDC claimed that it needed the data to give the agency "deeper insights into the pandemic as it pertains to human behavior."

The data itself was scrapped by Safegraph from cell phone location trackers. Not everyone has that feature turned on but tens of millions do. The CDC shelled out half a million dollars to get what they had, all of it gathered without any concern for ethics or privacy.

> Location data is information on a device's location sourced from the phone, which can then show where a person lives, works, and where they went. The sort of data the CDC bought was aggregated—meaning it was designed to follow trends that emerge from

> the movements of groups of people—but researchers have repeatedly raised concerns with how location data can be deanonymized and used to track specific people. The documents reveal the expansive plan the CDC had last year to use location data from a highly controversial data broker.

What this means is that the CDC was essentially monitoring if people went to get an illegal haircut, attended an illicit house party, or left the house after a 10 pm curfew. Or went to church. Or shopped at a nonessential store. It seems strange that we would have any such laws in the US regardless, and it is nothing short of an outrage that a government bureaucracy would pay a private-sector company for access to that in order to monitor your compliance.

And we can see here how this works. You get a phone and it includes apps that want to know your location, often for good reasons. You need a GPS. You want to see restaurants around you. You want to know the weather. People who push ads want them to be specific to where you are. So you leave location services on even when you could otherwise turn them off. This allows app companies to scrape vast information from your phone, mostly anonymous but not quite entirely.

This data then becomes available on the open market. The CDC becomes a customer, and why should any company hungry for cash refuse such an offer? Of course they should but too often revenue needs trump ethics in this world. The check arrives and out goes the data. In this way, the government has the means to spy on you nearly directly. And it does this without any legislative or judicial authorization.

This raises profound questions about deploying track-and-trace methods for a virus that is as prevalent as covid. It never held out any chance of controlling the spread, no matter what they say. It does introduce profound dangers of government surveillance of the citizenry to police people for compliance, which can very quickly become a means of political enforcement.

The damage is done already but it is wise to be aware now of what is possible. Much of the infrastructure was set up over these two years and it all still survives. There is every intention in place to deploy it all again if covid mutates again or if some other pathogen comes along. Lockdowns seem to be in disrepute among the public but the ruling class is still in love with them.

What can we learn from this fiasco?

1. Congress and the judiciary are not in control of government. Especially once there is an “emergency,” the administrative state believes itself to be an autonomous force, doing what it wants regardless of the constitution. There is almost no oversight.

2. Many private companies are no longer private at all. A main customer is the government and they adjust their operations to make their products marketable to them. They collect your data and sell it to the state. There is rarely anything in the terms of use of most apps that prevent that.

3. No matter how paranoid you are now, it is probably not enough. Pandemic control was a pretext for doing to the citizens what never would have been tolerated in normal times. The lockdowns are over but the aspiration to track and control us completely has just begun. The

years 2020 and 2021 were just trial runs for what they want to be permanent.

4. There are things you can do to protect yourself but it requires volition and focus. Indiscriminate use of mainstream applications is dangerous to both privacy and liberty.

5. What I've reported above already happened a year ago, so it is right to ask the question: what are they doing now? They got away with it then, a fact which only encourages more egregious behavior.

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram, Twitter and Facebook. Feel free to repost and share widely Global Research articles.

Jeffrey A. Tucker is Founder and President of the Brownstone Institute and the author of many thousands of articles in the scholarly and popular press and ten books in 5 languages, most recently Liberty or Lockdown. He is also the editor of The Best of Mises. He speaks widely on topics of economics, technology, social philosophy, and culture.

Featured image is from Shutterstock
