MERCOLA
Take Control of Your Health

Contact Tracing Apps Violate Privacy

Analysis by Dr. Joseph Mercola ✔ Fact Checked | February 24, 2023

STORY AT-A-GLANCE

- The Rockefeller Foundation's white paper, "National COVID-19 Testing Action Plan" lays out a strategic framework that is clearly intended to become part of a permanent surveillance and social control structure that severely limits personal liberty and freedom of choice
- Contact-tracing apps are a significant part of this scheme, and the Rockefeller plan clearly states that "Whenever and wherever possible data should be open," and that "privacy concerns must be set aside"
- The U.S. is rapidly adopting an artificial intelligence-driven mass surveillance system rivaling that of China, and legal and structural obstacles are being swept away under the guise of combating COVID-19
- Contact-tracing apps require you to keep your cellphone on your person throughout the day, giving thousands of third parties access to personal data
- Privacy protects people from interference, intervention and manipulation, and must be protected at all costs

From Dr. Joseph Mercola

Since COVID-19 first entered the scene, exchange of ideas has basically been outlawed. By sharing my views and those from various experts throughout the pandemic on COVID treatments and the experimental COVID jabs, I became a main target of the White House, the political establishment and the global cabal.

Propaganda and pervasive censorship have been deployed to seize control over every part of your life, including your health, finances and food supply. The major media are key players and have been instrumental in creating and fueling fear.

I am republishing this article in its original form so that you can see how the progression unfolded.

Originally published: May 15, 2020

Two days ago, I wrote about The Rockefeller Foundation's plan to test, track and trace all Americans — ostensibly to prevent COVID-19 from overwhelming us as we're again "allowed" to venture outside our front doors in limited capacity around the nation.

The Rockefeller Foundation's April 21, 2020, white paper,[1] "National COVID-19 Testing Action Plan — Strategic Steps to Reopen Our Workplaces and Our Communities," lays out a strategic framework that is clearly intended to become part of a permanent surveillance and social control structure that severely limits personal liberty and freedom of choice.

The Rockefeller plan calls for COVID-19 testing and tracing of 1 million Americans per week to start, incrementally ramping it up to 3 million and then 30 million per week (the "1-3-30 plan") over the next six months until the entire population has been covered.

Test results would then be collected on a digital platform capable of tracking all tested individuals so that contact-tracing can be performed when someone tests positive.

Contact-tracing apps are a significant part of this scheme, and the white paper[2] clearly states that "Whenever and wherever possible data should be open," and that "Some privacy concerns must be set aside for an infectious agent as virulent as Covid-19, allowing the infection status of most Americans to be accessed and validated in a few required settings and many voluntary ones."

Techno-Tyranny Steps Into Broad Daylight

As noted in The Last American Vagabond's article,[3] "Techno-Tyranny: How the U.S. National Security State Is Using Coronavirus to Fulfill an Orwellian Vision," the U.S. is rapidly adopting an artificial intelligence-driven mass surveillance system rivaling that of China, and legal and structural obstacles are now being swept away "under the guise of combating the coronavirus crisis."

Indeed, the Rockefeller plan doesn't even try to hide its draconian overreach and intent to permanently alter life and society as we know it. In the first half of the 20th century, George Orwell wrote a dystopian novel, "Nineteen Eighty-Four," in which the government controlled every aspect of a person's life, including their very thoughts.

Today, scientists seem intent on turning Orwell's nightmarish vision into reality, using the COVID-19 pandemic, national security and public health as their justification for doing so. Artificial intelligence — AI — is a key ingredient in this surveillance plot. Ironically, as noted by The Last American Vagabond:[4]

> *"Last year, a U.S. government body dedicated to examining how artificial intelligence can 'address the national security and defense needs of the United States' discussed in detail the 'structural' changes that the American economy and society must undergo in order to ensure a technological advantage over China, according to a recent document[5] acquired through a FOIA request.*
>
> *This document suggests that the U.S. follow China's lead and even surpass them in many aspects related to AI-driven technologies, particularly their use of mass surveillance.*
>
> *This perspective clearly clashes with the public rhetoric of prominent U.S. government officials and politicians on China, who have labeled the Chinese government's technology investments and export of its surveillance systems and other technologies as a major 'threat' to Americans' 'way of life.'[6]"*

The document[7] the article refers to was produced by the National Security Commission on Artificial Intelligence (NSCAI), a government organization created by the National Defense Authorization Act (NDAA) of 2018.

Its purpose is "to consider the methods and means necessary to advance the development of artificial intelligence (AI), machine learning and associated technologies to comprehensively address the national security and defense needs of the United States," and to ensure the U.S. maintains a technological advantage.

To that end, the NSCAI is pushing for an overhaul of the American way of life and economy in order to usher in a more comprehensive AI-driven surveillance apparatus.

Google Is a Major Player and Threat in This Arena

It is important to understand that Google has the greatest AI team in the world. To boost its powerbase, in 2014 Google purchased Deep Mind, an AI company that employed some of the world's leading AI experts at the time.[8]

One of those top-notch scientists was David Silver, who led the team that created the program Alpha Go, which subsequently defeated the world champion of the abstract boardgame, Go.[9] Most recently, Silver won the 2019 Association for Computing Machinery award for breakthrough advances in computer game-playing.[10]

Lex Fridman from MIT recently had a fascinating interview with Silver.[11] The reason I mention it is because this accomplishment is perceived by many as a great milestone. It established deep reinforcement learning as a strategy that will allow computers to rapidly outperform humans and rapidly implement advanced versions of the surveillance state.

So, not only does Google have the AI scientists, but they also have the largest computing platform in the world and a major lead in quantum computing, already establishing quantum supremacy late last year.[12]

We Cannot Afford To Be Naïve

The DW News video above reviews the rollout of COVID-19 contact tracing apps in various parts of the world and their approaches to privacy concerns. Germany, at

present, appears to be one of the nations that are most protective of their privacy rights. This makes perfect sense, considering its Nazi history.

Many Americans, on the other hand, do not have personal experience with the kind of human rights atrocities perpetuated in Nazi Germany, and fail to understand just how slippery the slope is.

Recent calls by American leaders to call police and snitch on their neighbors for failing to observe social distancing rules, for example, come straight from the authoritarian handbook, and there's simply no excuse for not recognizing and interpreting it at face value.

Rights and liberties are never simply handed to us. Every single human right and freedom you currently enjoy has been fought and paid for in blood, and unless we refuse tyranny from the very get-go, we'll eventually be forced to live under it or pay for our freedom with blood sacrifices yet again. We cannot afford to be naïve about where we're headed.

Contact Tracing Apps Violate Your Privacy

A May 4, 2020, Forbes article[13] by Simon Chandler points out that while contact-tracing apps "may be cryptographically secure," they still "threaten our privacy in broader and more insidious ways."

> *"On the one hand, cybersecurity researchers have already argued[14] that suitably determined and malevolent bad actors could correlate infected people with other personal info using the API. On the other, the Google-Apple API and any app based on it carry two much more general and dangerous privacy risks,"* Chandler writes.

What are some of these privacy risks? Well, for starters, contact-tracing apps require you to keep your cellphone on your person throughout the day, regardless of what you're doing.

Aside from whatever concerns people may have about electromagnetic field exposure from their cellphone being on their body while turned on — which is no small concern in and of itself — your cellphone also tracks and shares countless other data that is unrelated to the COVID-19 app.

As noted by Chandler, "A Washington Post study[15] from last year discovered around 5,400 (mostly app-based) data trackers on an iPhone, all of which were sending data back to third-parties," and "all of these companies have an interest in using that data to later influence and indirectly control your behavior ..."

Privacy Is About Preventing Interference and Manipulation

Chandler makes another very important point that many fail to remember when it comes to privacy:[16]

> *"Privacy actually gains most of its importance and value because it protects people from interference and intervention. You may want to keep your fondness for, say, ballet dancing private from your neighbors, because of the risk that they might mock your pastime and make you feel ashamed about wanting to be a ballet dancer.*
>
> *You worry that they will interfere — either directly or indirectly — with your ability to develop as a person according to your own awareness and conception of your best interests. Exactly the same thing goes for privacy in the context of smartphones and digital technology.*
>
> *It's not enough to avoid sharing your data with the 'wrong' people (as opposed to scores or hundreds of 'legitimate' third parties). You also need to avoid interference and intervention to have true privacy. And in encouraging people to have their smartphones with them all the time, coronavirus contact-tracing apps fail abjectly in this test."*

COVID-19 Tracing Apps Set Precedent for Behavior-Control

Contact tracing apps will also "normalize the concept of apps themselves directing and managing at scale how millions of people live and behave," Chandler points out. The app will notify you whenever you've come in close proximity of someone who tests positive for SARS-CoV-2 infection. You'll then be advised to self-isolate for a prescribed amount of time. As reported ty Chandler:[17]

> *"This is a massive problem for anyone concerned about the future of privacy and personal freedoms in the Digital Age. It would be one thing if any contact-tracing app could guarantee that a user had definitely been infected with the coronavirus. But there's a very strong likelihood that such apps will also send notifications to lots of people who haven't been infected ...*
>
> *Coronavirus contact-tracing apps will end up requiring thousands (if not millions) of people to quarantine themselves at home unnecessarily. So, in most cases, rather than preventing coronavirus infections from spreading, the only thing such apps will achieve is desensitizing the general public to giving up another chunk of their privacy and personal freedom."*

In other words, over time, people will get used to the idea of having their day-to-day activities predicated on what an app tells them to do. A virtually guaranteed result of this habituation is the handing over of personal judgment and discernment to an AI. "In the process, they'll suffer from the kind of outside interference with their behavior that privacy is meant to defend against," Chandler says.

Rockefeller Plan Is Not Limited to COVID-19 Tracing

The tracking system The Rockefeller Foundation is calling for in the U.S. also demands access to other medical data. According to its "National COVID-19 Testing Action Plan":[18]

> *"This infection database must easily interoperate with doctor, hospital and insurance health records in an essential and urgent national program to finally*

> *rationalize the disparate and sometimes deliberately isolated electronic medical records systems across the country ...*
>
> *On March 9, the Department of Health and Human Services (HHS) released two long-awaited final rules that would prohibit information blocking in health care and advance more seamless exchange of health care data. But publication in the Federal Register, necessary to activate the rules, has been inexplicably delayed. This delay must end."*

In other words, this plan is far more comprehensive than merely tracking COVID-19 cases. It's designed to replace the current system of "disparate and sometimes deliberately isolated electronic medical records systems across the country."

Will You Embrace Totalitarianism for False Sense of Security?

A small shred of hope still exists that enough Americans will see through this ruse. Oxford researchers estimate[19] that in in order for contact tracing apps to be effective, about 60% of any given population would need to participate.

According to a national poll[20,21] conducted by The Washington Post and the University of Maryland between April 21 and April 26, 2020, 3 in 5 Americans say they're either unable or unwilling to allow silent surveillance by a cellphone app, even in the name of public health.

One in 6 said they didn't have a smartphone. Even among Americans that have smartphones with the appropriate capabilities, about half said they would not participate.

According to The New York Times,[22] only 3% of residents in North Dakota had downloaded the state's contact tracing app as of April 29, 2020. The app was announced and released April 7, 2020.[23]

In Singapore, only 1 in 6 (20%) had downloaded the government's contact tracing app by April 1, 2020,[24] while 30% of Norwegians downloaded their government's app within the

first week of its release, according to The New York Times.[25]

In an effort to maintain some semblance of privacy protection, some nations, such as France, have decided to use "short-range Bluetooth 'handshakes' between devices" and keep the data on centralized servers, while others are opting to use GPS location data[26] and a variety of other systems. A May 5, 2020, article in TechCrunch describes the differences between some of them.[27]

As reported by BBC News,[28] Cannes, France, is also trialing surveillance monitoring software on buses and outdoor markets to keep tabs on social distancing compliance. According to the software developer, this surveillance complies with EU data privacy laws by not storing or transmitting any images or identifying data.

Cannes Mayor David Lisnard told BBC: "This technology doesn't identify people but just gives us mathematical analysis to meet people's needs." Still, if rules are breached, the AI will send an automatic alert to police and city authorities.

Apps Cannot Replace Conventional Disease Tracing

The World Health Organization, meanwhile, has noted that these types of apps still cannot replace old-fashioned disease surveillance and tracing measures. As reported by Reuters:[29]

> *"As countries begin easing lockdowns imposed to curb the spread of the virus, many hope to contain new clusters of infection through systematic contact tracing, helped by mobile phone apps and other technology.*
>
> *But [WHO's top emergency expert Dr. Mike] Ryan said these did not make more traditional 'boots-on-the-ground' surveillance redundant. 'We are very, very keen to stress that IT tools do not replace the basic public health workforce that is going to be needed to trace, test, isolate and quarantine,' he said ..."*

'Health Passports' Are in the Works

Aside from the Rockefeller Foundation's plan for the U.S., other nations are also proposing the rollout of various types of "health passports," the oft-repeated refrain being that without digital health certificates, it simply won't be safe to return to work and leisure.

May 5, 2020, TechCrunch reported[30] the rollout of a contact tracing app in the U.K., developed by the National Health Service. The first testing ground will be the Isle of Wight, which has a population of about 140,000. According to TechCrunch:

> *"The **NHS COVID-19** app uses Bluetooth Low Energy handshakes to register proximity events (aka 'contacts') between smartphone users, with factors such as the duration of the 'contact event' and the distance between the devices feeding an NHS clinical algorithm that's being designed to estimate infection risk and trigger notifications if a user subsequently experiences COVID-19 symptoms ...*
>
> *However there are major questions over how effective the tool will prove to be, especially given the government's decision to 'go it alone' on the design of its digital contacts-tracing system — which raises some specific technical challenges linked to how modern smartphone platforms operate, as well as around international interoperability with other national apps targeting the same purpose.*
>
> *In addition, the UK app allows users to self-report symptoms of COVID-19 — which could lead to many false alerts being generated. That in turn might trigger notification fatigue and/or encourage users to ignore alerts if the ratio of false alarms exceeds genuine alerts."*

What's more, while the app initially only stores contact events on each individual's device, once a user flags him or herself as having symptoms or testing positive, the contact data is uploaded to a central server that will store the data indefinitely, and from which it cannot be deleted.

This data may also be used for public health research, which again raises questions about privacy and the possibility of re-identification of individuals. May 4, 2020, The Guardian also reported on U.K. developments:[31]

> *"Tech firms are in talks with ministers about creating health passports to help Britons return safely to work using coronavirus testing and facial recognition. Facial biometrics could be used to help provide a digital certificate — sometimes known as an immunity passport — proving which workers have had Covid-19 ...*
>
> *The UK-based firm Onfido, which specializes in verifying people's identities using facial biometrics, has delivered detailed plans to the government and is involved in a number of conversations about what could be rolled out across the country ...*
>
> *Its proposals, which have reached pilot stages in other countries, could be executed within months ... The firm could use antibody tests — proving whether someone has had the virus — or antigen tests, which show current infections."*

Antigen Testing Cannot Ensure Safety

Why antigen testing is part of these kinds of "health passports" is a curious mystery, seeing how unreliable they are, not to mention the fact that testing for active infection is worthless unless you get retested on a regular basis. As I mentioned in my Rockefeller plan article, questions that have yet to be answered include:

- How often would you have to undergo testing? A negative test today may not be valid tomorrow, if you happen to come across someone who is infected between now and then. If regular retesting is not part of the plan, then the whole system is worthless as your infection status could change at any time.
- If you are in the vicinity of someone who tests positive in the near future and are told to quarantine for two weeks, will employers pay for that time off and guarantee you have a job to come back to afterward?

- What happens if you quarantine for two weeks but don't get sick and test negative for antibodies, then go out and happen across yet another person who ends up testing positive shortly thereafter? Will you be forced into quarantine again? Where does it end? And when?

Contact Tracing Apps May Cause More Problems Than They Solve

An April 27, 2020, article[32] by the Brookings Institute lays out some of the many problems inherent with contact tracing apps. It states, in part:

> *"We are concerned by this rising enthusiasm for automated technology as a centerpiece of infection control. Between us, we hold extensive expertise in technology, law and policy, and epidemiology. We have serious doubts that voluntary, anonymous contact tracing through smartphone apps ... can free Americans of the terrible choice between staying home or risking exposure.*
>
> *We worry that contact-tracing apps will serve as vehicles for abuse and disinformation, while providing a false sense of security ... We have no doubts that the developers of contact-tracing apps and related technologies are well-intentioned. But we urge the developers of these systems to step up and acknowledge the limitations of those technologies before they are widely adopted.*
>
> *Health agencies and policymakers should not over-rely on these apps and, regardless, should make clear rules to head off the threat to privacy, equity, and liberty by imposing appropriate safeguards ...*
>
> *Apps that notify participants of disclosure could, on the margins and in the right conditions, help direct testing resources to those at higher risk. Anything else strikes us as implausible at best, and dangerous at worst."*

The article goes on to highlight a number of risks, including the fact that contact tracing apps are imperfect proxies for exposure. They can easily trigger false positive alerts in situations where the possibility of transmission is extremely low, such as when the signal has traveled through a wall. People in different rooms are not at high risk of infection.

The apps also do not take into account the use of protective gear by the contacts. Also, the elderly, who might stand to gain the most protection from it, are the least likely to download the app. Even those who have the app may not always have the phone on them to catch all contacts, and people might not report symptoms and positive test results even if they get them.

"Even among true contact events, most will not lead to transmission," Brookings says, citing research showing that despite having about a dozen close contacts each day, the average person who is infected will only transmit the virus to two or three others throughout the entire course of their infection. Brookings continues:

> *"Because most exposures flagged by the apps will not lead to infection, many users will be instructed to self-quarantine even when they have not been infected. A person may put up with this once or twice, but after a few false alarms and the ensuing inconvenience of protracted self-isolation, we expect many will start to disregard the warnings ...*
>
> *Ultimately, contact tracing is a public health intervention, not an individual health one. It can reduce the spread of disease through the population, but does not confer direct protection on any individual.*
>
> *This creates incentive problems that need careful thought: What is in it for the user who will sometimes be instructed to miss work and avoid socializing, but does not derive immediate benefits from the system? ...*
>
> *And finally, the issue of malicious use is paramount — particularly given this current climate of disinformation, astroturfing, and political manipulation. Imagine an unscrupulous political operative who wanted to dampen voting*

participation in a given district, or a desperate business owner who wanted to stifle competition.

Either could falsely report incidences of coronavirus without much fear of repercussion. Trolls could sow chaos for the malicious pleasure of it. Protesters could trigger panic as a form of civil disobedience. A foreign intelligence operation could shut down an entire city by falsely reporting COVID-19 infections in every neighborhood. There are a great many vulnerabilities underlying this platform that have still yet to be explored."

Sources and References

- [1, 2, 18] The Rockefeller Foundation, National COVID-19 Testing Action Plan — Strategic Steps to Reopen Our Workplaces and Our Communities, April 21, 2020 (PDF)
- [3, 4] The Last American Vagabond April 20, 2020
- [5, 7] Chinese Tech Landscape Overview, NSCAI Presentation May 2019 (PDF)
- [6] Washington Examiner July 20, 2020
- [8] TechCrunch January 26, 2014
- [9] Association for Computing Machinery April 2020
- [10] Association for Computing Machinery April 1, 2020
- [11] YouTube April 3, 2020
- [12] Nature 574, 2019, 505–510
- [13, 16, 17] Forbes May 4, 2020
- [14] Wired April 17, 2020
- [15] Washington Post May 28, 2019
- [19] University of Oxford April 16, 2020
- [20] Washington Post-University of Maryland National Poll April 21-26, 2020
- [21] Washington Post April 29, 2020
- [22, 25] The New York Times April 29, 2020
- [23] Valley News April 7, 2020
- [24] StraitsTimes.com April 1, 2020
- [26] Reuters May 3, 2020
- [27, 30] TechCrunch May 5, 2020
- [28] BBC News May 4, 2020
- [29] Reuters May 4, 2020
- [31] The Guardian May 4, 2020
- [32] Brookings Institute April 27, 2020