MERCOLA
Take Control of Your Health

CDC Tracked Americans' Cell Phones During Lockdowns

Analysis by Dr. Joseph Mercola ✔ Fact Checked | June 02, 2022

STORY AT-A-GLANCE

- A Freedom of Information Act request to the CDC revealed documentation that the organization had freely received, and later purchased, location data with the stated intent of monitoring activity in curfew zones or visits to pharmacies
- A review of the documents also disclosed a list of 21 cases where the data could possibly be used, not all of which involved tracking COVID-related efforts. The data were gathered by SafeGraph after the company's code was installed in a variety of apps commonly downloaded to smartphones
- The data are reportedly anonymized, yet SafeGraph decided to no longer share data location about clinics that offer abortion services, which begs the question "Why?" if the data are anonymous?
- Google banned SafeGraph code in the Play Store in July 2021, just six months before four attorneys general filed a lawsuit after a three-year investigation showing Google has been secretly tracking people since 2014

If you've ever felt like Google knows what you're going to do before you know what you're going to do, it's because they are tracking you. If you're using any of Google's apps or products on your Android phone, iPhone or computer, you are likely being tracked. Internal documents[1] from the Centers for Disease Control and Prevention show your cell phone data was used to track your movements during lockdowns and vaccine campaigns.

CNET reports that some apps created by Google can store your location data and just opening the maps app or using a Google search will log your location and time.[2] Google analyzes the data to predict your behavior and sells the information to advertisers.

But advertisers are not the only ones interested in knowing where you are and what you're doing. As the pandemic unfolded in Australia,[3] officials decided not to take the word of their citizens. Instead, citizens are forced to download an intrusive app that uses facial recognition and geolocation to ensure they stay quarantined in their homes.

In October 2021, The Guardian reported that human rights groups were concerned that the data being collected in Australia could be used for "secondary purposes" and stored for longer than necessary. The Human Rights Law Center and Digital Rights Watch have expressed concern about the technology being used without privacy protections for their citizens.

The groups also expressed concerns that the information will be stored indefinitely rather than destroyed when there's no reason for it to be retained. China has taken the use of their citizens' data one step further as they have developed measures to keep citizens in line with the party rhetoric.[4]

Officially, the government is using facial recognition, shaming and brutality to enforce quarantines in the hope of achieving zero COVID cases, infections or deaths in the country. In other words, China appears to be operating under the misguided belief that COVID is not endemic and can be controlled.

Yet, this is a highly unlikely story for a country with advanced technology and science laboratories. More likely, China and Australia are using these draconian methods to force submission and obedience on their citizens. Internal documents reveal that the CDC may be in the early stages of something similarly tyrannical.

CDC Pays for Data to Track Your Phone

May 3, 2022, Vice[5] reported that they'd learned through a Freedom of Information Act request that the CDC had purchased cell phone data from the data broker SafeGraph. In

early 2020, SafeGraph announced in their online blog[6] that they'd made their "foot traffic data free for nonprofit organizations and government agencies at the local, state and federal level" — but, in addition, they also created "multiple new COVID-19 datasets and dashboards."

They did this, they said, "to play our part in the fight against the COVID-19 health crisis — and its devastating impact on the global economy."[7] One year later, SafeGraph, whose large investors include PayPal co-founder Peter Thiel and ex Saudi intelligence chief Turki bin Faisal Al Saud, began charging for the data and the CDC paid $420,000 to the company.[8]

The CDC said the data were "critical for ongoing response efforts, such as hourly monitoring of activity in curfew zones or detailed counts of visits to participating pharmacies for vaccine monitoring."[9] Zach Edwards is a cyber-security researcher who commented to Vice Motherboard in an online chat after reading the documents from the CDC:[10]

> *"The CDC seems to have purposefully created an open-ended list of use cases, which included monitoring curfews, neighbor-to-neighbor visits, visits to churches, schools and pharmacies, and also a variety of analysis with this data specifically focused on 'violence.'"*

In the documents obtained through the FOIA, the CDC described 21 cases in which they could potentially use the data that they had purchased. Although the data were purchased to ostensibly track COVID data, not all were related to these efforts and it's apparent someone was hoping to prove the effectiveness of CDC decisions through:[11]

- Examination of volume of mobile phones grouped in proximity each month and compare 2019 to 2020 data to see the impact of these orders. Project how much worse things would have been without the bans.
- Examination of the effectiveness of public policy on Navajo Nation.
- Research points of interest such as visits to pharmacies in a vaccine distribution plan or grocery stores.

- Research points of interest for physical activity and chronic disease prevention such as visits to parks, gyms, or weight management businesses.
- Exposure to certain building types, urban areas, and violence.

SafeGraph defended its actions and data release by claiming it is an aggregate of information rather than specific to individuals to prevent issues with user privacy. In the past, the company shared data on over 18 million cell phones they say were geographically representative.

They gather the data by asking or paying app developers to include the SafeGraph code. The location data is then funneled to SafeGraph, where they resell it or package the data into products. SafeGraph claims that the data is anonymous, yet Vice Motherboard found otherwise after purchasing location data for $200 that was not supposed to pinpoint specific devices.

Edwards pointed out the data could be identified down to a specific office and theoretically specific users could also be identified. This is not the first time the CDC has used the mobile cell phone network to gather data on the population. In 2010[12] they used it to identify population displacement and return after the earthquake in Haiti.

Their data analysis corresponded with a retrospective survey but was not reproduced in other natural disasters because of the limitations in gathering data from telecommunication companies. SafeGraph seems to have circumvented this issue.

Google Blocked SafeGraph

The concern that the location data may breach privacy was supported by SafeGraph's decision in May 2022 to no longer share location data about clinics that offer abortion services.[13] Despite the long-standing claim that the data were anonymized, the company thought it was "good that we were called out." and the decision was made "in light of potential federal changes in family planning access."

How is it that SafeGraph believes the data sold to the CDC was anonymized, yet earlier that month they agreed to stop selling location data near health clinics that offer abortion services? Is one more anonymous than the other?

The New York Post[14] reported an example of how data have been able to be de-anonymized when a Catholic priest from Wisconsin was forced to resign after a Catholic news site was able to link data from his cell phone to dating apps.

The Post[15] also reported that the internal documents from the CDC cell phone data revealed "extremely accurate insights related to age, gender, race, citizenship status, income and more."

June 2021, Google banned SafeGraph code from their Play Store. Any developers who had it installed were required to either remove their app or remove the code. Yet, this is likely not effective since, as Vice reports,[16] SafeGraph has also gotten location data from a spin-off company that also works with app developers.

The intent to track user data was announced early in the pandemic by Bill Gates, who had gone on record saying that life would not go back to normal until we had the ability to vaccinate the entire global population against COVID-19.[17] To that end, he pushed for disease surveillance and a vaccine tracking system that could ultimately involve embedding vaccination records in our body.

The Rockefeller Foundation is also working on coordinating efforts of social control by implementing tracking and tracing measures that clearly are meant to become permanent. April 21, 2020,[18] the Foundation released a white paper that called for testing and tracing all Americans using a national database that connects to other health records.

While these announcements are not obviously tied to data gathering by Google or other third parties, it's also naive to think they can accomplish those goals without initially integrating data from the largest data source in the world — Google.

Google Has Been Secretly Tracking People

Google's ban on SafeGraph code seems opposite to company policy and an interesting twist of events in 2021 since four attorneys general alleged in 2022 that the tech giant has secretly been tracking people without their knowledge or permission. Karl A. Racine, attorney general for the District of Columbia, said in a statement, "The truth is that contrary to Google's representations it continues to systematically surveil customers and profit from customer data."[19]

Racine led the complaints based on a three-year investigation that showed Google was recording movements even after users had indicated they didn't want their movement tracked by changing settings on their device. "Google falsely led consumers to believe that changing their account and device settings would allow customers to protect their privacy and control what personal data the company could access," Racine said.[20]

Racine initiated the investigation after a 2018 AP news report[21] revealed Google was tracking people's movements even when they opted out. His investigation found that these misleading claims regarding user privacy protection had been ongoing since at least 2014.[22] Yet, a Google spokesperson alleged that the lawsuit was based on "inaccurate claims and outdated assertions about our settings."[23]

The AP investigation[24] included a real-world example from privacy researcher Gunes Acar, whose location data was tracked to dozens of locations over several days and the data saved to his Google account. Acar had turned off the "location history" on his cell phone.

In the past, Google location data had been used in criminal cases, including a warrant issued by police in Raleigh, North Carolina, to track down devices in the area of a murder.[25]

It is reasonable to assume that Google has access to your location when your data and location are turned on. However, at issue is the company's continued tracking even when location history is turned off.

"If you're going to allow users to turn off something called 'location history,' then all the places where you maintain location history should be turned off," Jonathan Mayer, a

former chief technologist for the Federal Communications Commission's enforcement bureau, told the AP.[26] "That seems like a pretty straightforward position to have."

Aside from hiding location tracking under settings users wouldn't expect, like "Web & App Activity" — which is turned on by default — Google is accused of collecting and storing location information via Google services, Wi-Fi data and marketing partners, again after device or account settings had been changed to stop location tracking.[27]

Massachusetts and Google Force Installs Tracking App

CNBC reported[28] that efforts in Congress to monitor Big Tech have been stalled by "both partisan and inter-party squabbles," while state attorneys general have shown a united front on issues against Facebook and Google. When asked, Racine attributed the alignment to the relationship the AGs have with their constituents.[29]

> *"State attorney generals are the people's lawyers. And when acting as the people's lawyers, they're doing their best work. And they do their best work by frankly, engaging and listening to the residents of their jurisdictions."*

This remarkably resembles the way that Congressional men and women were elected to do their jobs. Another signal that Google's ban of SafeGraph code was not likely to protect user privacy was its partnership with the Massachusetts Department of Public Health and Apple to create a smartphone app called MassNotify.[30]

The app tracks and traces people in Massachusetts and advises users of others' COVID-19 status. The tool claimed to have been developed "with a focus on privacy."[31] But Massachusetts residents were surprised when the app suddenly appeared on their Android phones without consent "to alert users who may have been exposed to COVID-19."

Reportedly, the user must enable the feature for it to function, but the partnership with Google makes this claim suspect. In China, COVID-19 tracking apps have been used as surveillance tools in collaboration with its social credit system, raising red flags that this

force-installed app could be tracking residents' movements and contacts without their knowledge and consent.

The MassNotify app uses Google's and Apple's Bluetooth-based Exposure Notifications Express program that was first released in April 2020. The program can act as a blueprint from which states can implement their own tracking systems. Other states have required users to download the app, but MassNotify was integrated into the operating system of Android phones directly.

In a May 2020 Forbes article,[32] Simon Chandler pointed out that while contact tracing apps "may be cryptographically secure," they still "threaten our privacy in broader and more insidious ways," namely encouraging you to keep your cellphone with you at all times and tracking your whereabouts while you do, further "normalizing" the constant use of technology to dictate your freedoms and behavior.

As has been demonstrated by investigations and Google's actions, your smartphone can easily be used to track your location and possible actions. This information can then be used to make predictions about your behavior and the likelihood you'll make decisions that are for or against the current government dictates.

There are minimal steps left before people in currently "free" countries are living under constant surveillance, control and brutality as people in China and Australia find themselves. It is crucial to support your local and state government officials who support freedom.

Sources and References

- [1, 5, 7, 9, 10, 16] Vice Motherboard, May 3, 2022
- [2] CNET, February 23, 2022
- [3] The Guardian, October 13, 2021, Para 5-8
- [4] Washington Post, April 18, 2022
- [6] SafeGraph April 14, 2020
- [8] The Vaccine Reaction, May 17, 2022, Para 3
- [11] Vice Motherboard, May 3, 2022, Image
- [12] Centers for Disease Control and Prevention, February 15, 2019
- [13] Protocol, May 4, 2022

- [14, 15] New York Post, May 4, 2022
- [17] GatesNotes, April 30, 2020
- [18] The Rockefeller Foundation, National COVID-19 Testing Action Plan — Strategic Steps to Reopen Our Workplaces and [...], April 21, 2020 (PDF) Page 2
- [19, 20, 22, 23, 27] The New York Times, January 24, 2022
- [21, 24, 25, 26] AP News August 13, 2018
- [28, 29] CNBC, April 2, 2022
- [30] Mass.gov, Enable MassNotify on your smartphone
- [31] Mass.gov, Enable MassNotify on your smartphone para 1
- [32] Forbes Coronavirus Contact Tracing Apps May 4, 2020