MERCOLA
Take Control of Your Health

Google Force Installs Vaccine Tracking, Tracing on Your Phone

Analysis by Dr. Joseph Mercola ✔ Fact Checked

STORY AT-A-GLANCE -

- The Massachusetts Department of Public Health partnered with Google and Apple to create a smartphone app called MassNotify, which tracks and traces people, advising users of others' COVID-19 status
- Massachusetts residents were alarmed when the software appeared on their phones without their consent or notification, raising concerns over privacy and spyware
- 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
- Google is a surveillance agency and a censoring agency with the ability to restrict or block access to websites across the internet, thus deciding what you can and cannot see
- Peaceful protests work to protect personal privacy and freedom; if you're a Massachusetts resident and are unhappy that surveillance software was added to your cellphone without your consent, now's the time to speak out

The Massachusetts Department of Public Health partnered with Google and Apple to create a smartphone app called MassNotify, which tracks and traces people, advising users of others' COVID-19 status.

For a tool that claims to have been developed "with a focus on privacy,"[1] imagine Massachusetts residents' surprise when the app suddenly appeared on their Android

phones out of nowhere. In a review on the Google Play Store, one shocked parent said:[2]

> *"This installed silently on my daughter's phone without consent or notification. She cannot have installed it herself since we use Family Link and we have to approve all app installs.*
>
> *I have no idea how they pulled this off, but it had to involve either Google, or Samsung, or both. Normal apps can't just install themselves. I'm not sure what's going on here, but this doesn't count as 'voluntary.' We need information, and we need it now, folks."*

The official MassNotify site, operated by the Massachusetts Department of Public Health, makes no mention that the app will automatically show up on residents' phones without consent, stating only that MassNotify is a "new tool that works through smartphones, with a focus on privacy, to alert users who may have been exposed to COVID-19."[3]

Reportedly, the feature must be enabled by the user for it to function, but it's extremely disconcerting that the tool has been automatically added to people's phones, whether they intend to use it or not.

Residents Alarmed Over 'Spyware,' 'Government Overreach'

Android phone users were understandably alarmed when MassNotify appeared on their devices. The tool "doesn't have an app icon," one person reported on Google Play, "you have to go through settings and view all apps. This is a huge privacy and security overstep by [Gov. Charlie Baker] & Google."[4]

Other people also described it as "spyware," while a user on Hacker News wrote, "It's pure madness that Play Services comes with this sort of backdoor. This is clearly what I would consider a deliberate … vulnerability."[5]

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. Reviews on the Google Play Store poured in from alarmed citizens worried about **privacy violations**, with comments such as:[6]

- *"Automatically installed without consent. It has no icon, no way to open this and see what it even does, which is a huge red flag … I think it's spyware, phishing as the DPH (Department of Public Health)."*
- *"Force-installed with no authorization or approval. App is hidden on the device to prevent uninstallation. Government overreach and corporate complicity should never be tolerated."*
- *"Unethical breach of privacy and a forceful misappropriation of personal property … The degree to which my data is collected or distributed through it has not been disclosed neither in active nor inactive form … I can only conclude and caution others that it is disclosing your whereabouts and social contacts without permission."*

MassNotify 'Built Into Device Settings,' Difficult to Remove

When pressed for comment, Google released a statement to the media, but did not address the glaring issue of how or why the system was force-installed without users' consent. Instead, they only stated:[7]

> *"We have been working with the Massachusetts Department of Public Health to allow users to activate the Exposure Notifications System directly from their Android phone settings.*
>
> *This functionality is built into the device settings and is automatically distributed by the Google Play Store, so users don't have to download a separate app. COVID-19 Exposure Notifications are enabled only if a user proactively turns it on. Users decide whether to enable this functionality and whether to share information through the system to help warn others of possible exposure."*

The MassNotify app was released June 15, 2021, marking the 29th state to launch an app using Google and Apple's Bluetooth-based Exposure Notifications Express program.

The software framework was first released in April 2020,[8] with the goal of allowing users who test positive for COVID-19 to report their results, which then sends out an alert to anyone whose phone crossed paths with the positive case and may have been exposed. The Exposure Notifications Express program acts as a blueprint from which states can implement their own tracking systems without having to develop their own individual apps.

While other states have required users to download an app to use the system, MassNotify was integrated directly into the operating system of Android phones.[9] "The contact-tracing feature does not work unless a user manually activates it, but you also can't get rid of the software," the Boston Globe reported. "(Meanwhile, Apple added the feature to iPhones months ago, with iOS 13.)."[10]

Massachusetts Urges Residents to Enable MassNotify

The Massachusetts Department of Public Health is urging residents to enable MassNotify on their cellphones, with Dr. Catherine Brown, state epidemiologist, stating that they're hoping at least 15% of the state's population, or more than 1 million people, will opt-in and noting that it could be most useful for those frequenting large workplaces or university campuses.[11]

Once you opt-in, anonymous codes are shared with other MassNotify users via your phone's Bluetooth. If within 14 days, you come in close contact — within 6 feet for at least 15 minutes[12] — with someone who tests positive, you'll be notified. If you test positive, you're expected to "easily and anonymously notify others to stop the spread of COVID-19."[13]

The system is working in connection with the Massachusetts Department of Public Health, which will send a text message with a verification link to those who test positive for COVID-19. The link allows users to share their test result and notify other

MassNotify users of their exposure. For those who haven't opted in to the tool, the link also serves as a tool "to help you enable MassNotify on your phone for future use."[14]

Unprecedented, Broad Privacy Risks Uncovered

It's ironic that the Massachusetts Department of Public Health states that MassNotify is not a contract tracing app,[15] yet it's based on technology developed by Apple and Google that was previously known as the "Privacy-Preserving Contact Tracing Project"[16] and is now referred to as the Exposure Notifications API (application programming interface).

In a May 2020 Forbes article by Simon Chandler, he points out that while contact tracing apps "may be cryptographically secure," they still "threaten our privacy in broader and more insidious ways":[17]

> *"On the one hand, cybersecurity researchers have already argued[18] 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."*

First the apps only work if you keep your cellphone with you at all times, with Bluetooth enabled. "Straight away, this is a massive privacy loss," Chandler notes. "As shown by numerous studies and investigations, smartphones and many of the apps on them track your locations, aside from recording — and sharing — whatever data you enter into them."[19]

The other risk is that it's one more way of "normalizing" something that's entirely abnormal — the constant use of technology to dictate your freedoms and behavior. "… [W]hile we're used to ads attempting to prod our consumer behavior, contact-tracing apps will normalize the concept of apps themselves directing and managing at scale how millions of people live and behave," Chandler pointed out.[20]

Remember, if you receive a notification that you've been in close contact with someone who tested positive, you'll be expected to quarantine. Many will undoubtedly be doing so

unnecessarily, as they won't end up sick, which means they've just given up 14 days of freedom for no reason.

And what happens if you finish quarantining only to go out in public and be notified of an exposure again? Another 14 days in isolation? Further, this seemingly innocent invasion has nefarious consequences. As Chandler put it:[21]

> *"Users will get used to the idea of an app telling them when to stay at home and when to go out. Basically, they'll become more habituated to delegating judgement over how they should behave to apps and digital technology."*

Google's Manipulation Techniques Are Well Known

Google has been called a dictator with unprecedented power because it relies on techniques of manipulation that have never existed before in human history, according to Robert Epstein, a Harvard trained psychologist who is now a senior research psychologist for the American Institute of Behavioral Research and Technology, where for the last decade he has helped expose **Google's manipulative and deceptive practices**.

They're not only a surveillance agency — think about products like Google Wallet, Google Docs, Google Drive and YouTube — but also a censoring agency with the ability to restrict or block access to websites across the internet, thus deciding what you can and cannot see.

Google has also infiltrated education with its Google classrooms, usage of which has skyrocketed during the pandemic, but many aren't aware that even their children are being tracked. The attorney general of New Mexico filed a suit against Google for its educational tools in its classroom suite, helping to "**break through the fog**," Harvard professor Shoshana Zuboff said:[22]

> *"[The suit is] identifying the huge amounts of data that they're taking about kids, how they track them across the internet are they integrate it with all the other*

Google streams of information and have it as a foundation for tracking those children all the way through their adulthood."

Google also backs **Profusa**,[23] which has developed an injectable biosensor that allows a person's physiology to be examined at a distance via smartphone connectivity. On a larger scale, Google, Amazon, Twitter and other major tech companies are also tied to the "**military-industrial-intelligence-media complex**," to quote Edward Curtin from Off-Guardian.[24]

All provide invaluable surveillance and censorship functions, and without them the **totalitarian control system** we now find ourselves caught in wouldn't be possible.

Mass Protests Can End Privacy Invasions

As we've seen in the case of vaccine passports, peaceful protests work to protect personal privacy and freedom. The Pentagon also pulled the plug on Lifelog — a database project aimed at tracking the minutiae of people's entire existence for national security surveillance purposes[25] — February 4, 2004, in response to backlash over privacy concerns.[26] (Although that same day, Facebook was launched.[27])

If you're a Massachusetts resident and are unhappy that surveillance software was added to your cellphone without your consent, now's the time to speak out. The end goal here isn't about tracking COVID-19 cases in your hometown. Vaccine passports or any other type of tracking and tracking device or certification system are part of a much larger plan to implement a global social credit system based on 24/7 electronic surveillance to ensure compliance.

This will expand to include not just COVID-19 infection and vaccination status but also other medical data, basic identification records, financial data and just about anything else that can be digitized and tracked.

It could mean the beginning of the end for freedom as we know it, unless everyone, everywhere recognizes the danger and takes action. Peaceful protest and civil

disobedience — simply not complying with tracking apps, mask mandates, social distancing, lockdowns, vaccination or anything else — can be a key part of the solution.

Sources and References

- [1, 3, 13] Mass.gov, Enable MassNotify on your smartphone
- [2] The National Pulse June 19, 2021
- [4, 5, 6, 7] ZeroHedge June 22, 2021
- [8] The Verge September 1, 2020
- [9, 10] Boston Globe June 22, 2021
- [11, 12] 10 WJAR June 21, 2021
- [14, 15] Mass.gov, Learn more about MassNotify
- [16] Apple.com, Privacy-Preserving Contact Tracing
- [17, 19, 20, 21] Forbes May 4, 2020
- [18] Wired April 17, 2020
- [22] YouTube June 22, 2020
- [23] Profusa, Our Team
- [24] Off-Guardian February 14, 2021
- [25] Military.com February 4, 2004
- [26] Rapture Ready FAQ: Lifelog project
- [27] History Facebook Launches February 4, 2004