MYTH BUSTING

Legend #1 - The legislature is utilizing the Trace Together application to track or keep an eye on each resident's whereabouts.

No, the Trace Together application doesn't gather any area information and its absolutely impossible for the administration to find your whereabouts with this application. The application utilizes Bluetooth innovation to trade associations with close by gadgets that have the application. The application just can show associations among gadgets, and not their areas. Moreover, the logs remain in your telephone. Ought to MOH need the logs for contact following, they will look for your agree to impart the logs to them.

Legend #2 - With the Trace Together application running on my cell phone that is Bluetooth empowered, anybody, including the legislature, can hack into my telephone and concentrate all data in the telephone.

Trace Together utilizes Bluetooth, a short-run distributed interchanges innovation that is pervasive in cell phones and gadgets today. It can just transmit flags inside a scope of

around 10 meters. Utilizing Trace Together is the same as interfacing different gadgets or wearables to your telephone through Bluetooth. Guarantee that your telephone working framework is refreshed to utilize Bluetooth securely. It is hard for anybody to draw near enough to you, and utilize a PC to remove data from your telephone without you taking note.

Legend #3 - If I download Trace Together and offer agree to all in-application capacities, I am basically permitting the Ministry of Health (MOH) and the administration to gather and access all my own information, just as the information in my telephone.

At the point when you set up Trace Together, you might be requested your portable number. This is the main individual information that MOH will hold about you, and it is put away in an exceptionally made sure about server together with an irregular anonymous user ID that is connected to your portable number. The security level of this server is as high as those servers that store other authority data.

All MOH will get is your telephone number. Business applications for messages, web perusing

and film observing gather a bigger number of information about you than this application.

When the application is running on your telephone, it will make a transitory ID, produced by scrambling the User ID with a private key that is held by MOH. The transitory ID is then traded with close by telephones, and restored normally, making it unthinkable for anybody to recognize or connect the brief IDs to you. The transitory ID must be unscrambled by MOH, with MOH's secretly held key. Your telephone will store the transitory IDs from close by telephones, together with data about the close by telephone's model, Bluetooth signal quality, and time. This data is put away locally on your telephone, and not sent to MOH, except if you are contact followed.

These measures shield clients from noxious on-screen characters who may try to spy and track co-operations after some time.

Fantasy #4 - If MOH contact-followed to me and requests that I transfer the information put away in the Trace Together application, the Ministry can likewise extricate whatever other information that they need from my telephone.

At the point when a Trace Together client is an affirmed COVID-19 case and consents to transfer the information sign in the Trace Together application to MOH, MOH will unscramble the impermanent IDs in the client's application utilizing its secretly held key, and get a rundown of telephone

numbers from the transferred information log. Each telephone number will just have the data identified with the Bluetooth signal quality and time data. That is all the data that MOH will get from the client's application log. In light of the sign quality and time data, MOH will at that point figure out which gadgets were in physical vicinity with the affirmed case.

Fantasy #5 - I don't wish to download this Trace Together application which will expand the danger of an information break on my telephone.

The Trace Together application doesn't build the danger of an information break on your telephone. Given the application's security and protection defends, the danger of an information spill from your telephone because of Trace Together is low. By downloading the application, you can tap on innovation to upgrade contact following – a key mainstay of Singapore's battle against COVID-19. The decision is yours to make.

Legend #6 - All data in the Trace Together application is transferred onto a server that faces an unending danger of being hacked into.

Aside from your versatile number, at the purpose of

enrollment, all information gathered through the Trace Together application is put away locally in your telephone in a scrambled structure. It isn't transferred to any focal server. The information will never be gotten to, except if you have been affirmed as a COVID-19 patient. The MOH contact following group will at that point approach you for unequivocal endorsement to get to the information in your application, and it is moved to private stockpiling that isn't presented to the Internet.

Fantasy #7 - Other Trace Together clients can see my telephone number.

Versatile numbers are not uncovered to other Trace Together clients. Just brief IDs, produced by scrambling the User ID with a private key that is held by MOH, are traded between telephones. Your portable number stays mystery and isn't traded with other cell phones. As an additional layer of insurance, the brief IDs are revived routinely. Regardless of whether you could unscramble the brief IDs, you would even now not have the option to acquire the versatile quantities of individuals you have been in contact with.

Legend #8 - Even after I uninstall the Trace Together application, my versatile number and the randomized User ID will stay in the server until the end of time.

Once Trace Together is uninstalled or the application's usefulness debilitated, all association information gathered on your telephone will be lost. You can likewise demand for your portable number and User ID to be expelled from the server by sending an email to support@tracetogether.gov.sg. This promptly renders all information gathered by other Trace Together telephones about their communications with you trivial, in light of the fact that that information can never again be related with you.

When contact following exercises stop, the Trace Together application will incite clients to deactivate its usefulness.