DPEX
DATA PROTECTION EXCELLENCE NETWORK

STRAITS INTERACTIVE

Webinar
A Comparative Review of Contact Tracing Apps in ASEAN Countries

Data Protection Excellence Network
May 28, 2020

Objectives

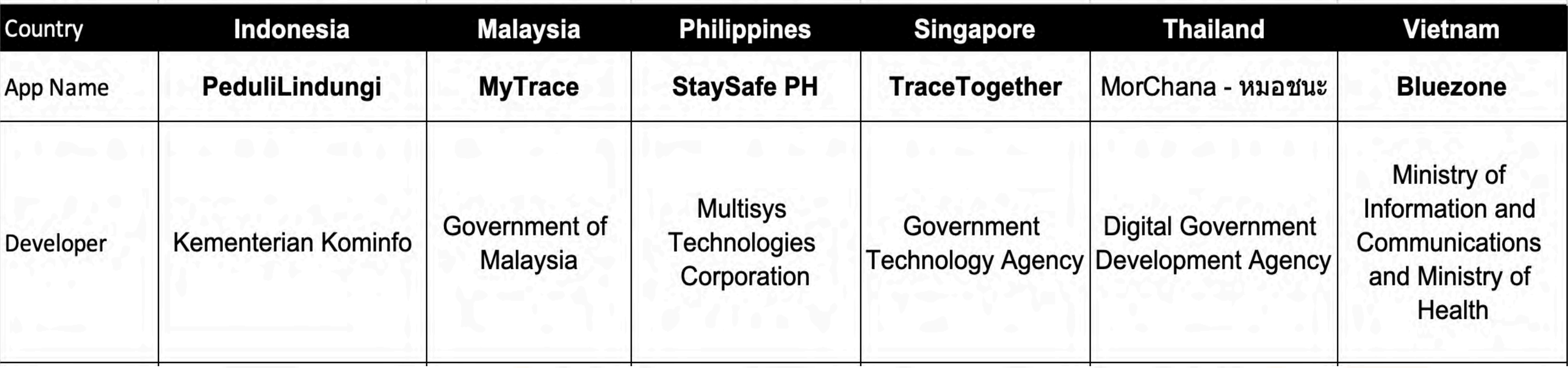
- Determine how privacy-invasive contact tracing apps are in ASEAN countries
- Address privacy and surveillance concerns of these users in the region

Benchmarking the ASEAN Contract Tracing app against the GPEN survey parameters

In 2014 GPEN (Global Privacy Enforcement Network) did a global privacy sweep that assessed:

- the types of permissions sought by mobile apps
- whether those permissions exceeded what would be expected based on the app's functionality
- most importantly, how the app explained to consumers why it wanted the personal data and what it planned to do with it

Android downloads



Country	Indonesia	Malaysia	Philippines	Singapore	Thailand	Vietnam
App Name	**PeduliLindungi**	**MyTrace**	**StaySafe PH**	**TraceTogether**	MorChana - หมอชนะ	**Bluezone**
Developer	Kementerian Kominfo	Government of Malaysia	Multisys Technologies Corporation	Government Technology Agency	Digital Government Development Agency	Ministry of Information and Communications and Ministry of Health

Use of Permissions

Every mobile phone has an ‘operating system’, most commonly the Android operating system (Google) or the iOS (Apple) operating system.

The vast majority of mobile phones are ‘Android phones’ and they have two ‘permissions’ categories:

- **Normal permissions**: these permissions do not directly risk the user’s privacy

- **Dangerous permissions**: these permissions give the app access to the user’s personal data in their mobile phone, such as contacts and SMS messages, as well as certain system features, such as the camera.

  Privacy laws do not allow the relevant personal data to be collected, used or disclosed unless the user gives explicit consent by ‘accepting’ the request for permission to do so.

Permissions	Bad	Good
Device & app history - Read sensitive log data - Retrieve system internal state - Read your web bookmarks and history - Retrieve running apps	- Ability to read read sensitive log data. - Other apps may store usernames and passwords in them — in plain text. - *Anything that says it's "sensitive" should be a tip-off.*	- This permission allows an app to read log data from other apps to perform a certain function.
Identity - Find accounts on the device - Read your own contact card (example: name and contact information) - Modify your own contact card - Add or remove accounts	- The app may discover all your Google Accounts and, together with other profile information, allow a hacker to abuse the information.	- Allows app to prepopulate your email address, first name, last name and phone number from your contact card during registration. - If user has Google Sign-In or a Google Wallet account on the device, the app can also use these permissions to prepopulate the email address. - Also used for signing in using Google+ account and to pay using Google Wallet.

Permissions	Bad	Good
Phone • directly call any phone numbers • read call log • read phone status and identity • re-route outgoing calls • write call log	• An app that asks to read your call log can now gain permission to reroute outgoing calls and make phone calls without asking you.	• The app requests access to make phone calls directly from the app - useful in situations such as a Taxi App.
Camera • take pictures and videos	• An app that has permission to take pictures and videos (for example, a camera app) can now gain the permission to record audio.	• The App lets individuals use the phone's camera to take photos (e.g. real estate) or scan (e.g. credit card) instead of manually typing in your payment information that will be sent to the server of the service.
Microphone • record audio	• The app could listen to you when you use other apps or when your device’s screen is off.	• Apps that need mic would use the voice recognition feature.

Permissions	Bad	Good
Calendar • add or modify calendar events and send email to guests without owner’s knowledge • read calendar events plus confidential information	• Can read all your appointments where many items could be private and confidential. Those with malicious intent could even modify or delete entries.	• If app includes calendaring function, you can conveniently add an appointment or follow-up on one.
SMS • edit your text messages (SMS or MMS) • read your text messages (SMS or MMS) • receive text messages (MMS) • receive text messages (SMS) • send SMS messages	• An app that only needs to receive text messages can now gain the permission to send SMS messages in the background, potentially also costing you money.	• When signing for a service, a company may send a 4-digit verification code, via SMS, to the mobile number. The "Receive SMS" permission allows the app to look for that incoming SMS message and automatically verify that the service has the correct mobile number.

Permissions	Bad	Good
Photos/Media/ Files • read the contents of your USB storage • modify or delete the contents of your USB storage	• The app can read the contents of your USB storage or SD card. It can also format your entire external storage device.	• Certain functions (mapping or image libraries) in the app use these permissions to allow the relevant map data, image, document (e.g. loan agreement) to be saved to your phone's external storage, like SD cards. By saving data locally, your phone doesn't need to re-download the same data every time you use the app.
Storage • read the contents of your USB storage • modify or delete the contents of your USB storage		
Location • approximate location (network-based) • precise location (GPS and network-based)	• **The app can now gain permission to track your exact location with your device's GPS. / Fine GPS Location & Coarse Network-based Location: The former can identify your location within several feet, the latter within a block or so.** • If the app has nothing to do with geo-location, it's probably reporting where you are to an ad server somewhere.	• Allows app to facilitate pick up (ride sharing), trip history in receipts, calculate distance between two points, locate e.g. ATMs. • Perfectly legitimate when the app in question has a mapping utility function.

TraceTogether Review

Kevin Shepherdson (FIP, CIPP/E, CIPP/A, CIPM, CIPT, GRCP)

Lyn Boxall (FIP, CIPP/E, CIPP/A, CIPM, GRCP, GRCA)

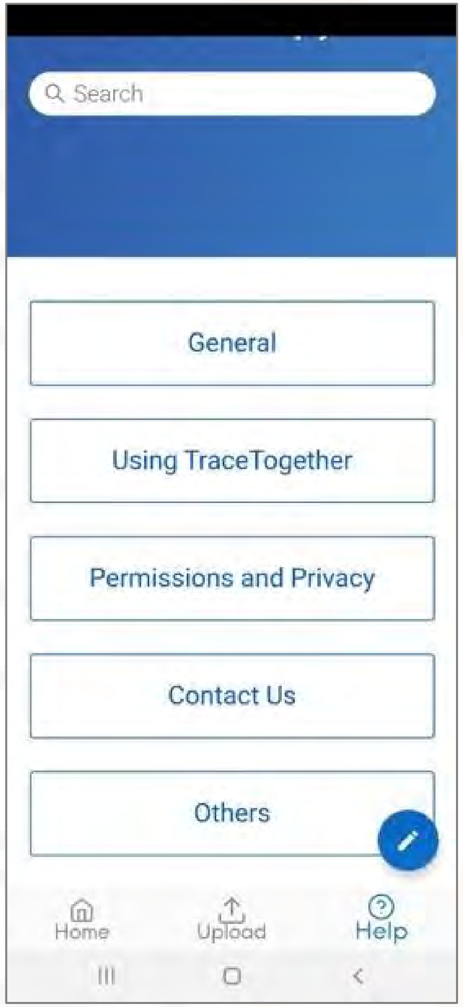
TraceTogether

Objectives of TraceTogether

The objectives of the TraceTogether app are to:

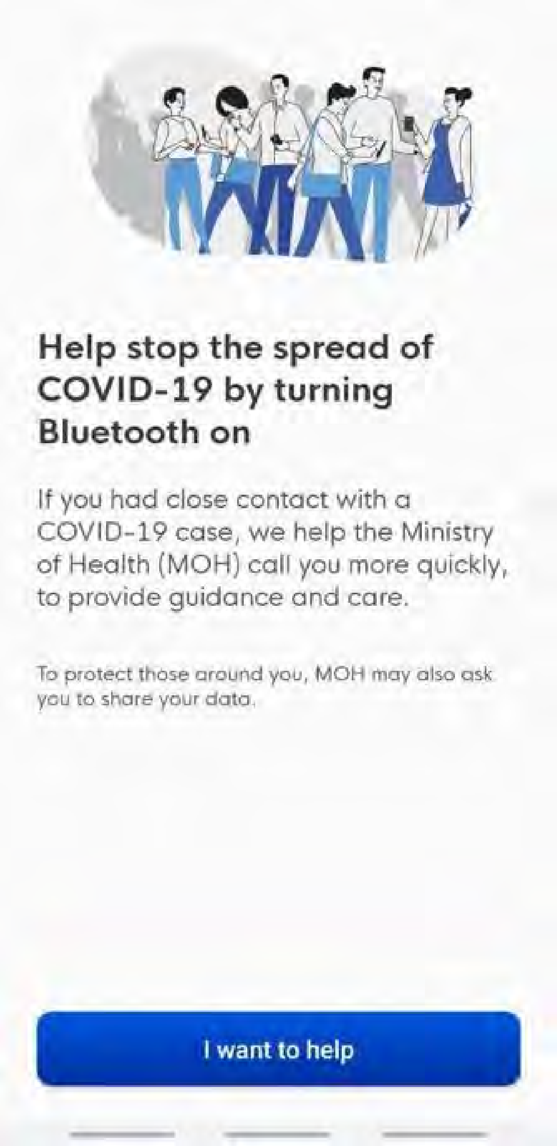
- allow users to ‘proactively help’ in contact tracing (by downloading the app and consenting to participate in the contact tracing process)

- support ongoing COVID-19 preventative efforts by speeding up and simplifying contact tracing while simultaneously making it more thorough



How TraceTogether works

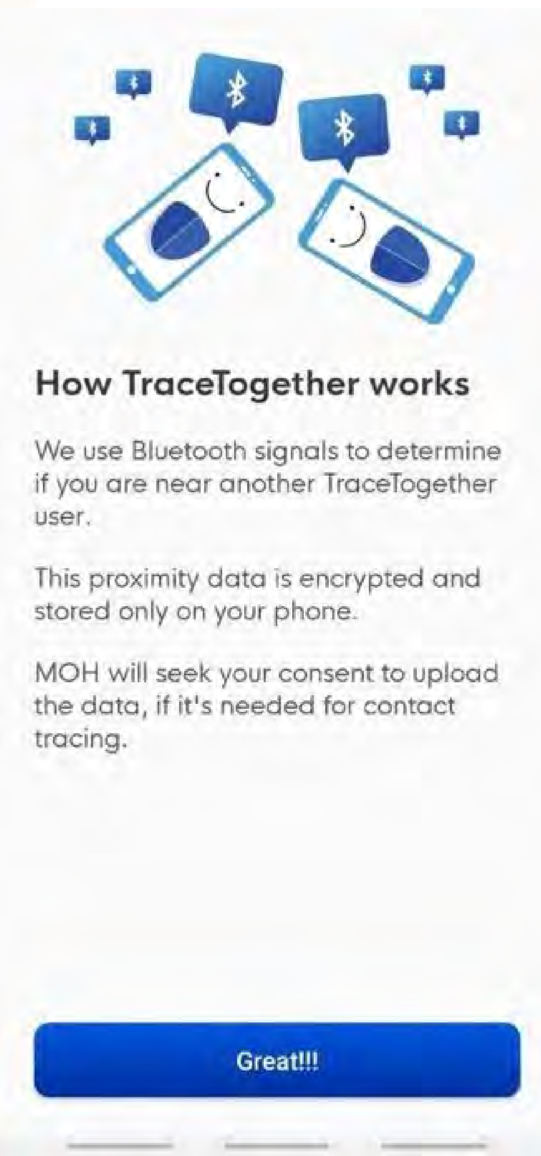
- User downloads the app and registers their mobile phone number.
- The app assigns a random anonymised User ID to the user’s mobile phone to identify it uniquely – for example, 9I8VPeQeWDofj39c8dPySoUXLqh2.
- A Temporary ID is generated by encrypting the User ID.
- User’s mobile phone uses short-distance Bluetooth signals to exchange the Temporary ID of their own mobile phone with the Temporary ID of any other user in ‘close proximity’.
- ‘Close proximity’ information is stored in the mobile phone of the TraceTogether app user for 21 days on a rolling basis.



Help stop the spread of COVID-19 by turning Bluetooth on

If you had close contact with a COVID-19 case, we help the Ministry of Health (MOH) call you more quickly, to provide guidance and care.

To protect those around you, MOH may also ask you to share your data.



How TraceTogether works

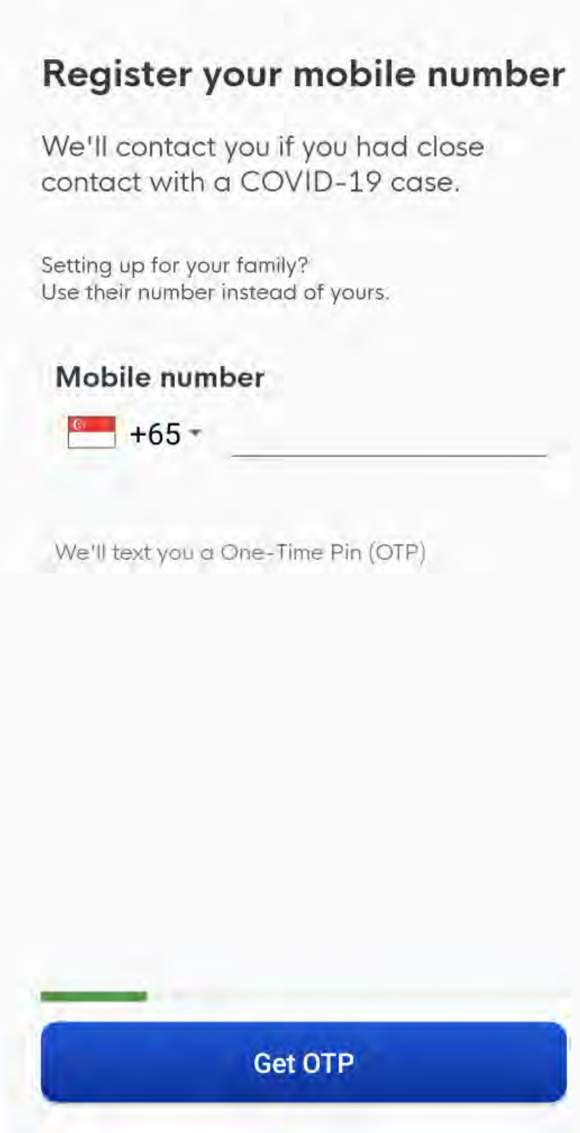
We use Bluetooth signals to determine if you are near another TraceTogether user.

This proximity data is encrypted and stored only on your phone.

MOH will seek your consent to upload the data, if it's needed for contact tracing.

How TraceTogether works

- The next stage happens only if:
  - a user of the TraceTogether app falls ill with COVID-19 or
  - the mobile phone of a user is found to have been in ‘close proximity’ with a COVID-19 case)
- MOH decrypts the user’s Temporary ID, revealing their User ID and phone phone number to MOH.
- MOH will seek the user’s consent to share their ‘close proximity’ information for the past 21 days with MOH.
- The user (like anyone else linked to infected cases) is required by law to assist in contact tracing irrespective of whether the individual uses the TraceTogether app.
- If they refuse to do so they may be prosecuted under the Infectious Diseases Act.



Register your mobile number

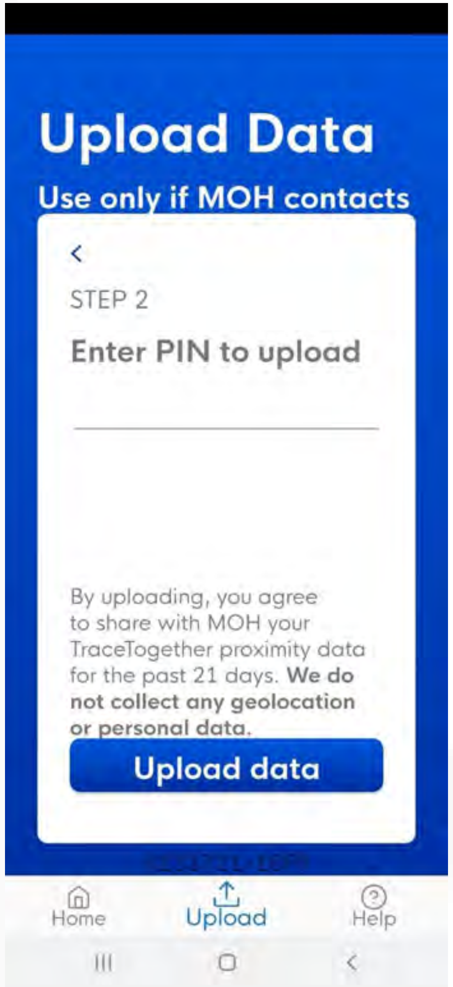
We'll contact you if you had close contact with a COVID-19 case.

Setting up for your family?
Use their number instead of yours.

Mobile number

+65

We'll text you a One-Time Pin (OTP)



Upload Data

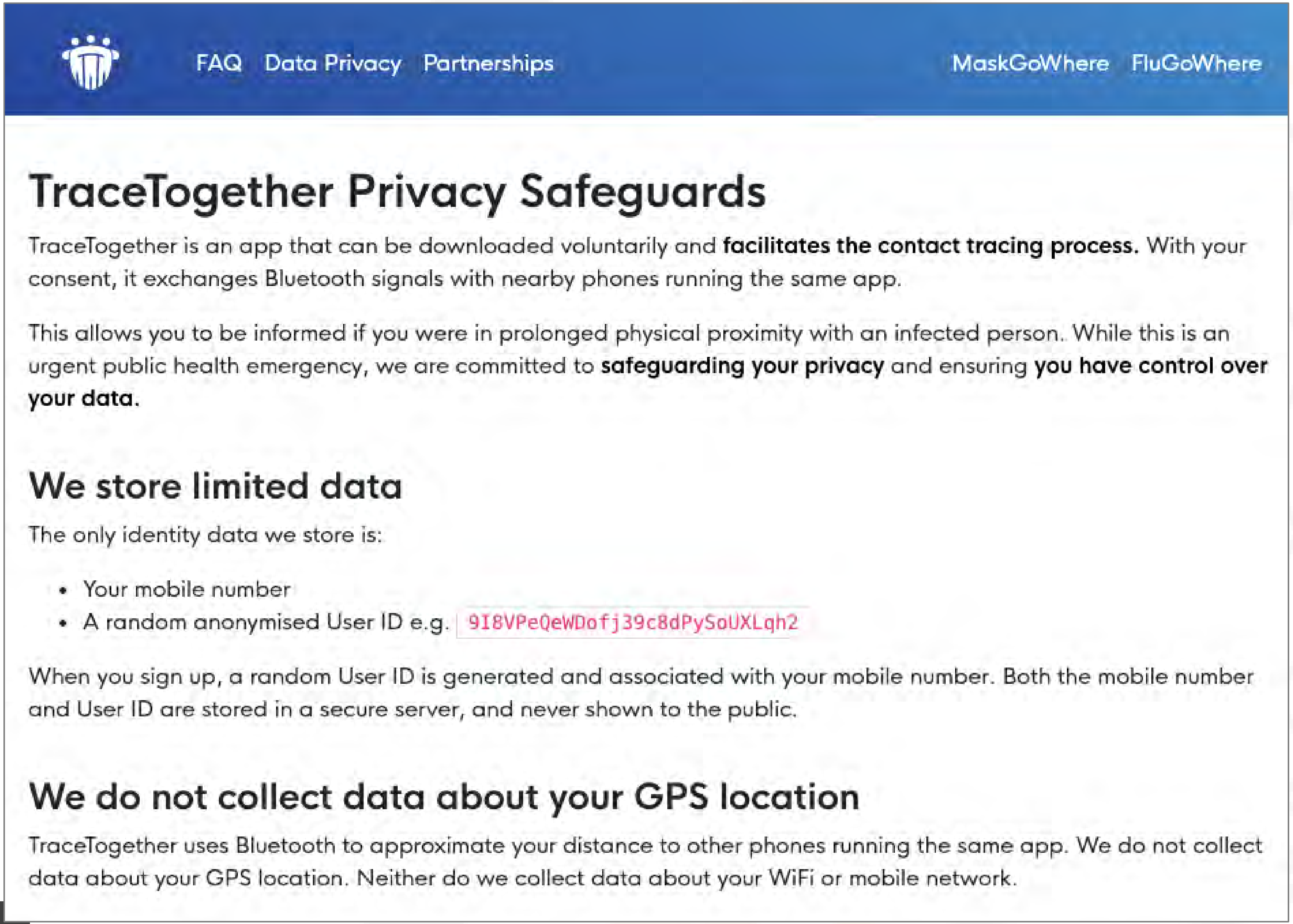
Use only if MOH contacts

STEP 2

Enter PIN to upload

By uploading, you agree to share with MOH your TraceTogether proximity data for the past 21 days. **We do not collect any geolocation or personal data.**

Privacy Notice



TraceTogether Privacy Safeguards

TraceTogether is an app that can be downloaded voluntarily and **facilitates the contact tracing process.** With your consent, it exchanges Bluetooth signals with nearby phones running the same app.

This allows you to be informed if you were in prolonged physical proximity with an infected person. While this is an urgent public health emergency, we are committed to **safeguarding your privacy** and ensuring **you have control over your data.**

We store limited data

The only identity data we store is:

- Your mobile number
- A random anonymised User ID e.g. `9I8VPeQeWDofj39c8dPySoUXLqh2`

When you sign up, a random User ID is generated and associated with your mobile number. Both the mobile number and User ID are stored in a secure server, and never shown to the public.

We do not collect data about your GPS location

TraceTogether uses Bluetooth to approximate your distance to other phones running the same app. We do not collect data about your GPS location. Neither do we collect data about your WiFi or mobile network.

- Privacy statement clearly states how personal data is processed.
- ”We store Limited data” – Mobile Phone number and random anonymised User ID.
- Addresses concerns about data in phone and other phone identities.

Overview of Permissions Used

Dangerous permissions used in TraceTogether

Photos/Media/ Files	• read the contents of your USB storage • modify or delete the contents of your USB storage
Storage	• read the contents of your USB storage • modify or delete the contents of your USB storage
Location	• approximate location (network-based) • precise location (GPS and network-based)
<u>Normal Permissions</u>	• receive data from Internet • access Bluetooth settings • full network access • prevent device from sleeping • view network connections • pair with Bluetooth devices • run at startup

Use of Permissions

Photos/Media/Files/Storage

- We can see that TraceTogether seeks permission to:
- modify or delete the contents of the USB storage in a user’s mobile phone
- read the contents of a user’s USB storage in their mobile phone

Justification: permissions are sought so that the app can store ‘close proximity’ information for 21 days on a rolling basis. This means that the ‘close proximity’ information can be read if it becomes necessary to trace the user’s contacts.

Use of Permissions

Photos/Media/Files/Storage

The privacy statement in the TraceTogether app says that:

- ‘Data about phones near you is stored only on your phone. If a user gets infected with COVID-19, he/she has the option to give MOH access to his/her TraceTogether data.’

- ‘When you grant MOH access to your TraceTogether data, this data will be used solely for contact tracing of persons possibly exposed to COVID-19.’

Use of Permissions

Location

According to the privacy statement for the TraceTogether app:

- ‘TraceTogether uses Bluetooth to approximate your distance to other phones running the same app. We do not collect data about your GPS location. Neither do we collect data about your WiFi or mobile network.’

<u>The statement about location is inconsistent</u> with the permissions listed (for which consent is sought by the app when downloading it):

- approximate location (network-based)
- precise location (GPS and network-based)

Use of Permissions

Location

- This inconsistency arises because:
  - Location permissions are mandatory when Bluetooth technology is used on an Android phone.
  - It is an outcome of how the Bluetooth technology works - the location permission is required so that ‘close proximity’ information can be collected.

- Confirmation that the app does NOT collect and store the location data used in relation to the ‘close proximity’ information.

- Neither the privacy statement nor the help documentation make this clarification, which could be confusing to a non-technical user.

	Singapore
PRIVACY COMMUNICATIONS	TraceTogether
Apps with concerns regarding pre-installation privacy communications	**No Issues**
Apps with excessive permissions based on sweeper's understanding of app's functionality	**No Issues**
Apps with privacy communications not well tailored to small screen	**No Issues**

OVERALL PRIVACY MARKS	TraceTogether
0 = No privacy information, other than permissions	
1 = Privacy information not adequate; sweeper does not know how information will be collected, used and disclosed	
2 = Privacy information somewhat explains the app’s collection, use and disclosure of personal information; however, sweeper still had questions about certain permissions	
3 = Privacy information clearly explains how app collects/uses/discloses personal information; sweeper is confident in his/her knowledge of app’s practices	Yes

MyTrace Malaysia Review

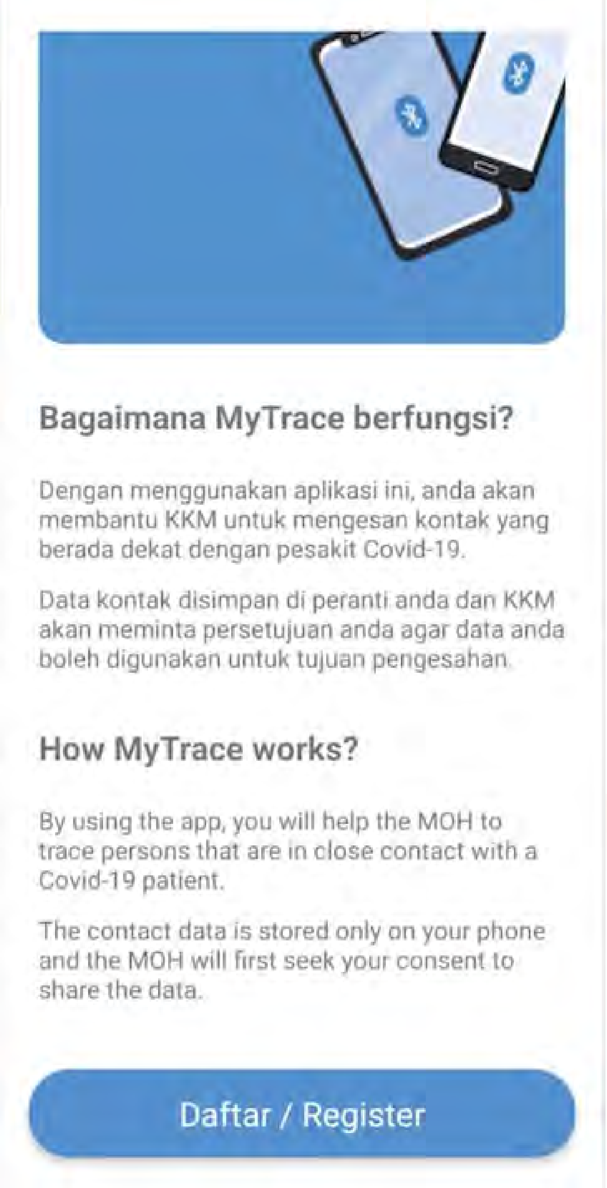
Ben Shepherdson (CIPM, Infosec & GDPR (Exin), GRCP)

Objectives of MyTrace

The objectives of the MyTrace app are to:

- Help the health authority to manage the COVID-19 outbreaks. MyTrace adopts a community-driven approach where participating devices exchange proximity information whenever an app detects another nearby device with MyTrace installed.

- The app enables identification of people who have been in close proximity to an infected person.



Bagaimana MyTrace berfungsi?

Dengan menggunakan aplikasi ini, anda akan membantu KKM untuk mengesan kontak yang berada dekat dengan pesakit Covid-19.

Data kontak disimpan di peranti anda dan KKM akan meminta persetujuan anda agar data anda boleh digunakan untuk tujuan pengesahan.

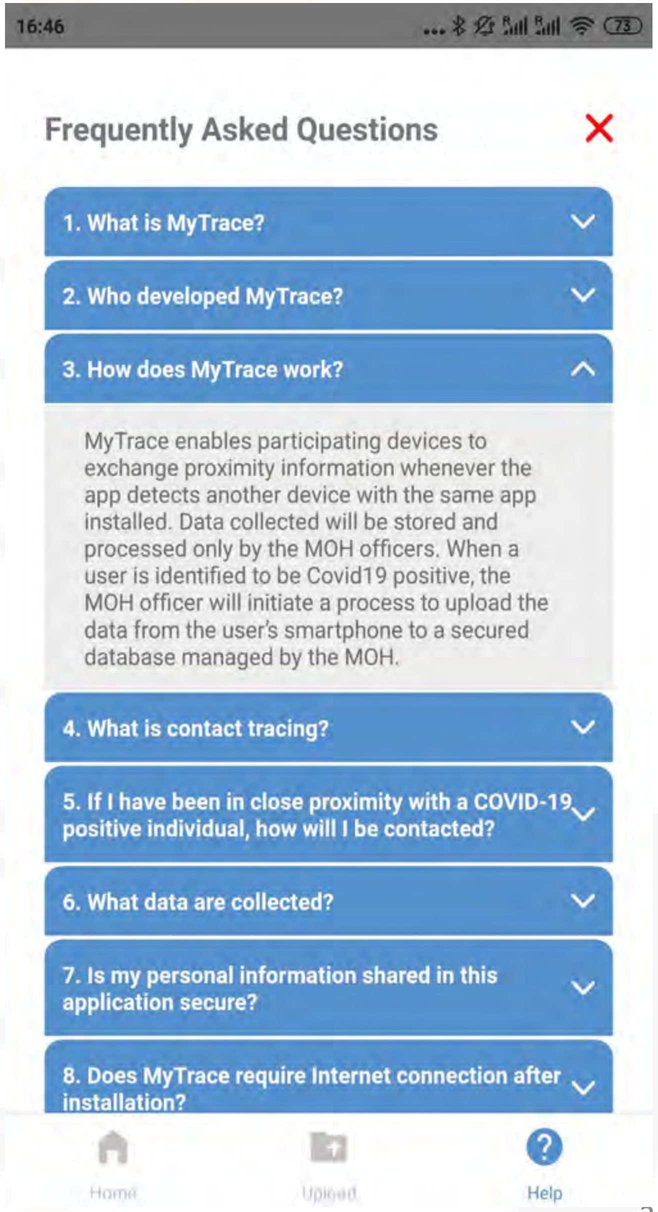
How MyTrace works?

By using the app, you will help the MOH to trace persons that are in close contact with a Covid-19 patient.

The contact data is stored only on your phone and the MOH will first seek your consent to share the data.

How MyTrace works

- User downloads the app and registers their mobile phone number assisted with an OTP
- The app assigns a Unique User ID to the user’s mobile phone to identify it
- User’s mobile phone uses short-distance Bluetooth signals to exchange participating devices proximity information whenever an app detects another nearby device with MyTrace installed
- ‘Close proximity’ information is stored in the users mobile phone of the MyTrace app user for 21 days on a rolling basis.



Frequently Asked Questions

1. What is MyTrace?

2. Who developed MyTrace?

3. How does MyTrace work?

MyTrace enables participating devices to exchange proximity information whenever the app detects another device with the same app installed. Data collected will be stored and processed only by the MOH officers. When a user is identified to be Covid19 positive, the MOH officer will initiate a process to upload the data from the user’s smartphone to a secured database managed by the MOH.

4. What is contact tracing?

5. If I have been in close proximity with a COVID-19 positive individual, how will I be contacted?

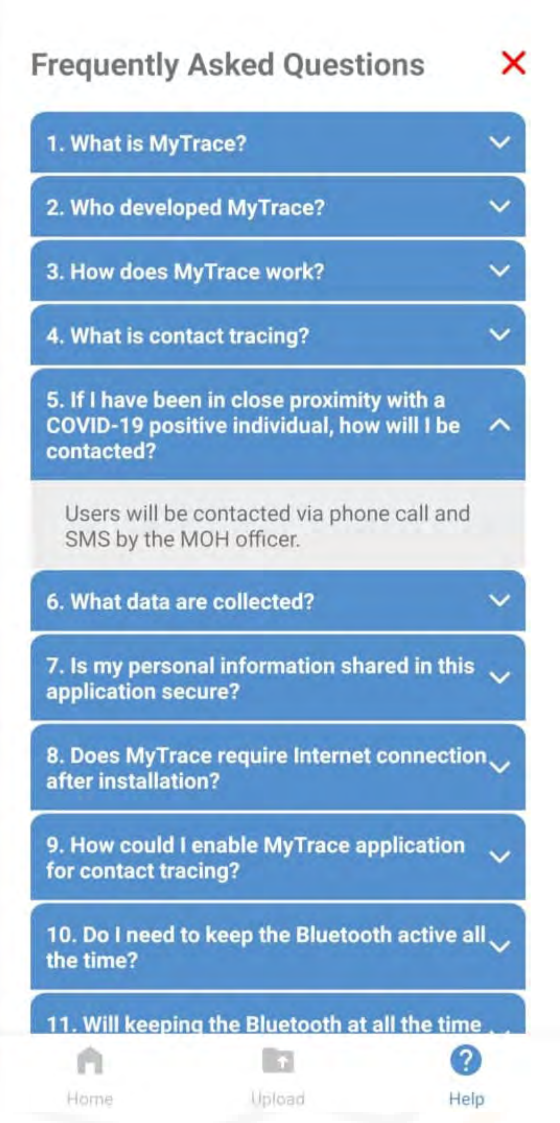
6. What data are collected?

7. Is my personal information shared in this application secure?

8. Does MyTrace require Internet connection after installation?

How MyTrace works

- Data collected will be stored and processed only by the MOH officers.
- When a user is identified to be a COVID-19 positive, the MOH officer will initiate a process to upload the data from the user’s smartphone to a secured database managed by the MOH
- MOH will contact the user via phone call and SMS. User will require to provide the unique verification code to MOH Officer.

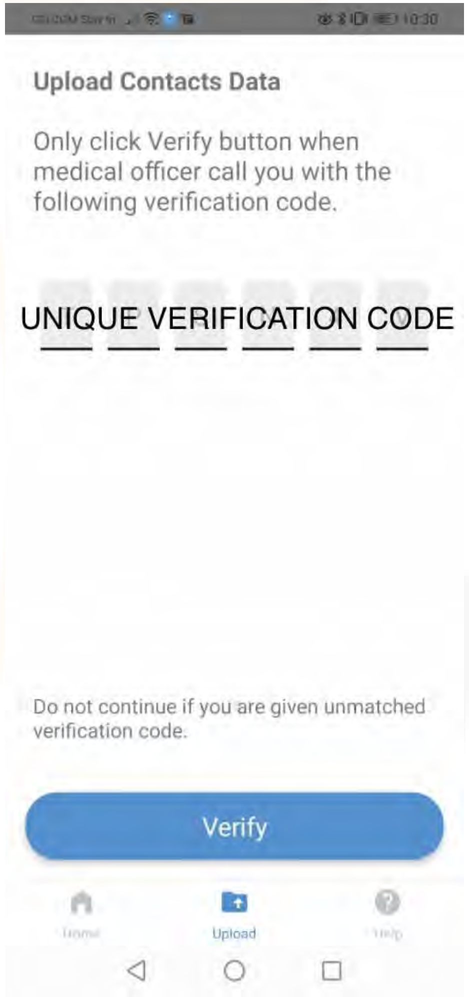


Frequently Asked Questions

1. What is MyTrace?
2. Who developed MyTrace?
3. How does MyTrace work?
4. What is contact tracing?
5. If I have been in close proximity with a COVID-19 positive individual, how will I be contacted?

Users will be contacted via phone call and SMS by the MOH officer.

6. What data are collected?
7. Is my personal information shared in this application secure?
8. Does MyTrace require Internet connection after installation?
9. How could I enable MyTrace application for contact tracing?
10. Do I need to keep the Bluetooth active all the time?
11. Will keeping the Bluetooth at all the time



Upload Contacts Data

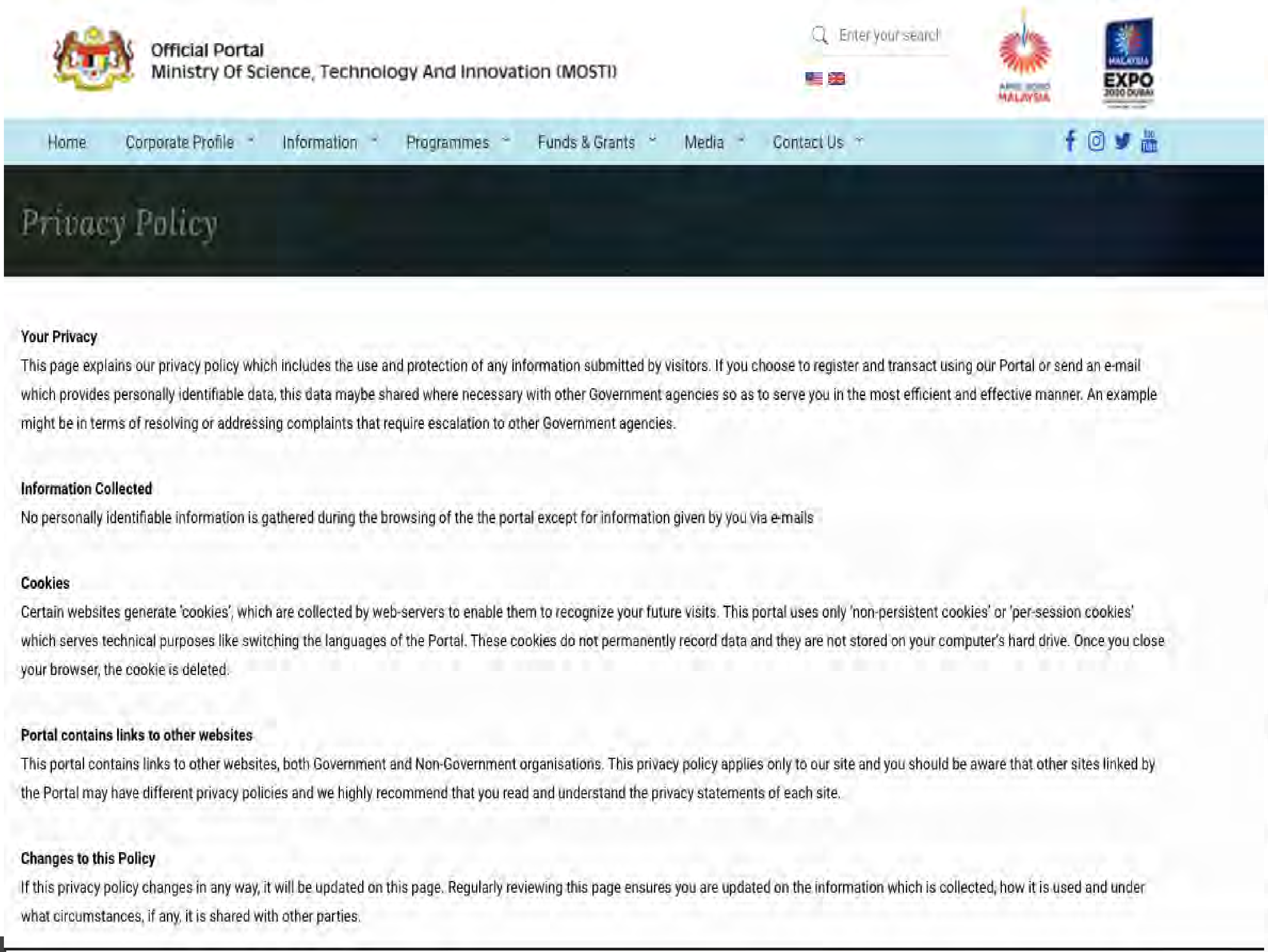
Only click Verify button when medical officer call you with the following verification code.

UNIQUE VERIFICATION CODE

Do not continue if you are given unmatched verification code.

Verify

Privacy Notice



Your Privacy

This page explains our privacy policy which includes the use and protection of any information submitted by visitors. If you choose to register and transact using our Portal or send an e-mail which provides personally identifiable data, this data maybe shared where necessary with other Government agencies so as to serve you in the most efficient and effective manner. An example might be in terms of resolving or addressing complaints that require escalation to other Government agencies.

Information Collected

No personally identifiable information is gathered during the browsing of the the portal except for information given by you via e-mails

Cookies

Certain websites generate 'cookies', which are collected by web-servers to enable them to recognize your future visits. This portal uses only 'non-persistent cookies' or 'per-session cookies' which serves technical purposes like switching the languages of the Portal. These cookies do not permanently record data and they are not stored on your computer's hard drive. Once you close your browser, the cookie is deleted.

Portal contains links to other websites

This portal contains links to other websites, both Government and Non-Government organisations. This privacy policy applies only to our site and you should be aware that other sites linked by the Portal may have different privacy policies and we highly recommend that you read and understand the privacy statements of each site.

Changes to this Policy

If this privacy policy changes in any way, it will be updated on this page. Regularly reviewing this page ensures you are updated on the information which is collected, how it is used and under what circumstances, if any, it is shared with other parties.

- Privacy statement does not state how personal data is processed.
- *No specific information relating to mobile app permissions*
- In the app under the FAQs page, the app informs user that the "data collection and the usage in this app will be in accordance with the government's information security standards"

- ***App does not notify user or ask for user consent for use of permissions.***

Overview of Permissions Used

Dangerous permissions used in MyTrace

Device & app history	• retrieve running apps
Photos/Media/ Files	• read the contents of your USB storage • modify or delete the contents of your USB storage
Storage	• read the contents of your USB storage • modify or delete the contents of your USB storage
Location	• approximate location (network-based) • precise location (GPS and network-based)
Normal	• receive data from Internet • view network connections • pair with Bluetooth devices • access Bluetooth settings • full network access • run at startup • prevent device from sleeping

Use of Permissions

Device & App History

We can see that MyTrace seeks permission to:

- retrieve running apps

No indication of the reason in Privacy notice and FAQs.

The presumption here is that the reason for this permission is to check on *the version* to ensure the app functions properly and whether an update is required.

Use of Permissions

Photos/Media/Files/Storage

We notice that MyTrace seeks permission to:

- modify or delete the contents of the USB storage in a user’s mobile phone
- read the contents of a user’s USB storage in their mobile phone

Justification: permissions are sought so that the app can store ‘close proximity’ information. This means that the ‘close proximity’ information can be extracted if it becomes necessary to trace the user’s contacts. There is no mention of retention period in the app or privacy notice.

*based on an interview with BFM and the minister on May 8, information is stored for 21 days

Use of Permissions

Photos/Media/Files/Storage

The FAQs in the MyTrace app says that:

- ‘Data about phones near you is stored only on your phone. If a user gets infected with COVID-19, he/she will be contacted by MOH to provide MOH access to his/her MyTrace data.’ This is done via MOH providing a matching unique verification code with the user’s device.

- ‘When you grant MOH access to your MyTrace data, this data will be used solely for contact tracing of persons possibly exposed to COVID-19.’

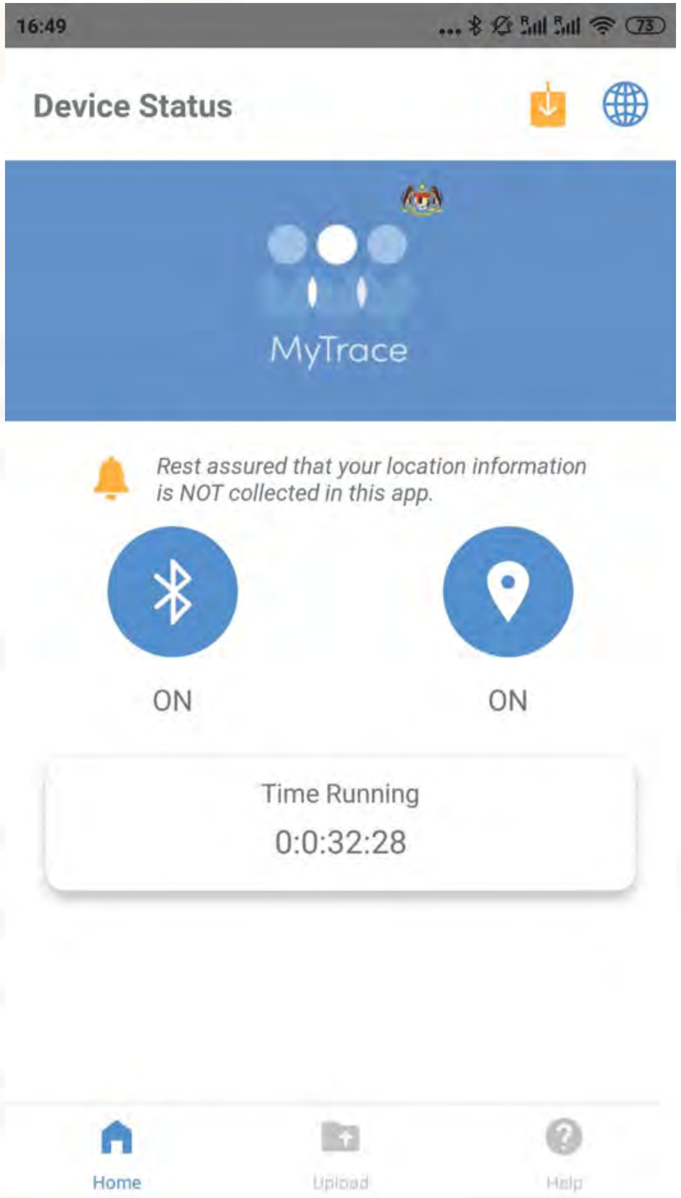
Use of Permissions

Location

According to the app and FAQ for the MyTrace app:

- ‘MyTrace uses Bluetooth via Relative Signal Strength Indicator(RSSI) and your approximate distance to other phones running the same app.

Under permissions, Location information is used. For Bluetooth technology to work, the location permission is required so that ‘close proximity’ information can be collected.



16:49

Device Status

MyTrace

Rest assured that your location information is NOT collected in this app.

ON

ON

Time Running

0:0:32:28

	Malaysia
PRIVACY COMMUNICATIONS	MyTrace
Apps with concerns regarding pre-installation privacy communications	Yes. There isn’t any communications about the privacy concerns i.e. permissions.
Apps with excessive permissions based on sweeper’s understanding of app’s functionality	Potentially Yes – relative to the purpose. Device Apps & Device permissions allows app to identify all apps running in the background. Privacy notice doesn’t clarify.
Apps with privacy communications not well tailored to small screen	Once installed, privacy communications are well informed ie permissions are clearly mentioned but not reflected in privacy Notice

OVERALL PRIVACY MARKS	MyTrace
0 = No privacy information, other than permissions	No. There is no information in privacy notice as well as terms and conditions.
1 = Privacy information not adequate; sweeper does not know how information will be collected, used and disclosed	
2 = Privacy information somewhat explains the app’s collection, use and disclosure of personal information; however, sweeper still had questions about certain permissions	
3 = Privacy information clearly explains how app collects/uses/discloses personal information; sweeper is confident in his/her knowledge of app’s practices	

PeduliLindungi Review

Andi Pramawijaya Sar

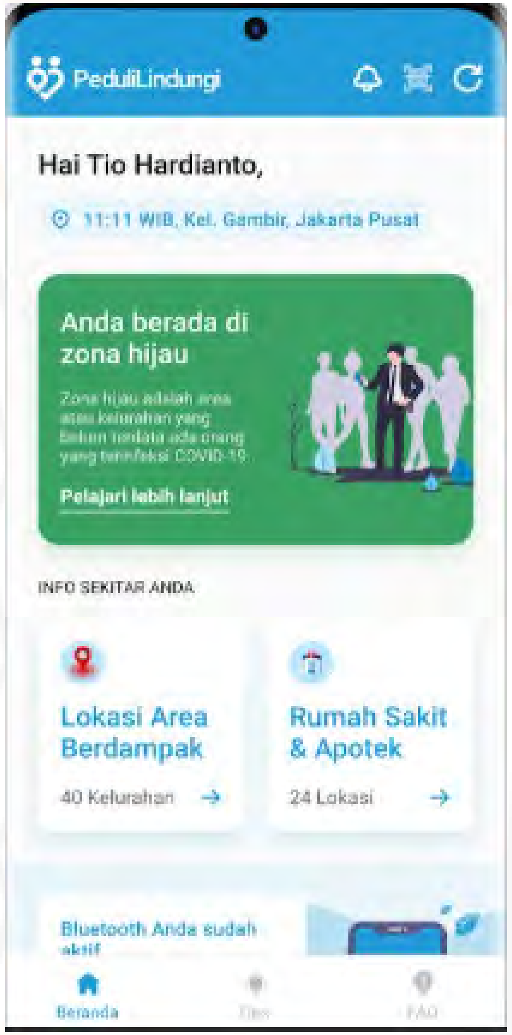
(Master candidate in Data Protection)

PeduliLindungi

Objectives of PeduliLindungi

The objectives of the PeduliLindungi app are to:

- stop the transmission of COVID-19 in Indonesia (conduct health surveillance by means of tracking, tracing, warning and fencing)
- bolster contact-tracing effort to track down cases and suspected patients - it relies on concern and community participation to share location data with each other while travelling so that tracing of the contact history with sufferers of COVID-19 can be done



PeduliLindungi

Hai Tio Hardianto,

11:11 WIB, Kel. Gambir, Jakarta Pusat

Anda berada di zona hijau

Zona hijau adalah area atau kelurahan yang belum terdata ada orang yang terinfeksi COVID-19

Pelajari lebih lanjut

INFO SEKITAR ANDA

Lokasi Area Berdampak
40 Kelurahan →

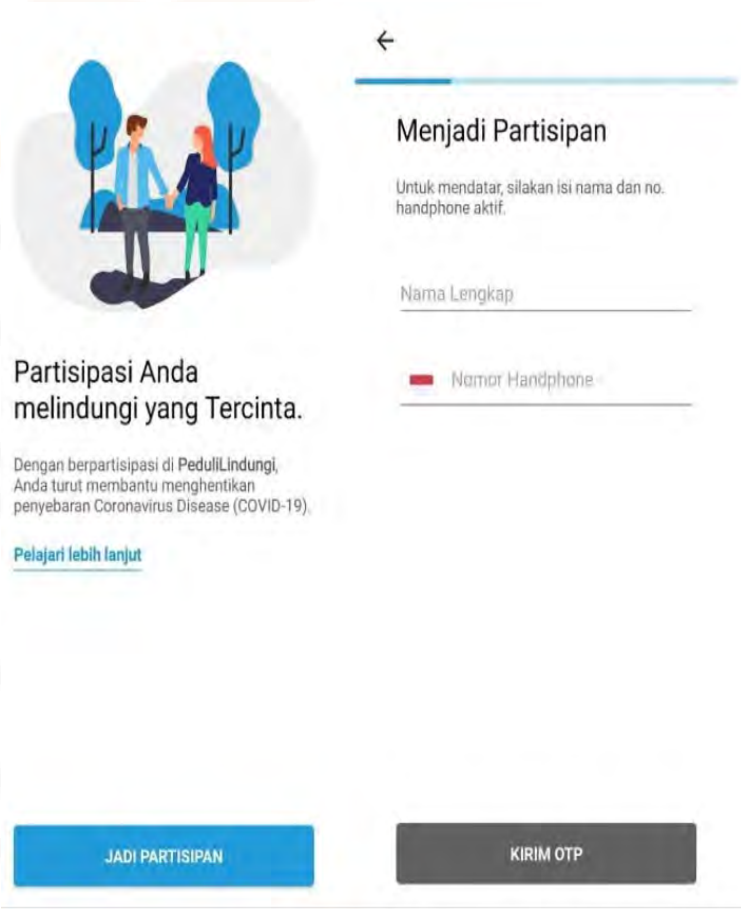
Rumah Sakit & Apotek
24 Lokasi →

Bluetooth Anda sudah aktif

How PeduliLindungi works

- User downloads the app and registers their complete name and mobile phone number.
- The app will ask the user’s consent to activate his/her mobile phone’s Bluetooth and Location information.
- When a user is in the vicinity of another user whose data has been uploaded to PeduliLindungi, the app enables an anonymous exchange of identities – the anonymous IDs data will be stored within a vulnerable period of 14 days.

- If a user is found to have been in close proximity with confirmed or suspected cases under surveillance, the app will identify them.
    - For example, a user with COVID-19 is confirmed by the health worker. According *to the Terms and Conditions, the* system will search the anonymous IDs that have been recorded in ‘close proximity’ within the last 14 days. Therefore, health-workers can inform other app users who who had been in contact with the infected person.
    - In short, this contact history information will be used to conduct tracing when one of the users is tested positive for COVID-19



Partisipasi Anda melindungi yang Tercinta.

Dengan berpartisipasi di **PeduliLindungi**, Anda turut membantu menghentikan penyebaran Coronavirus Disease (COVID-19).

Pelajari lebih lanjut

Menjadi Partisipan

Untuk mendatar, silakan isi nama dan no. handphone aktif.

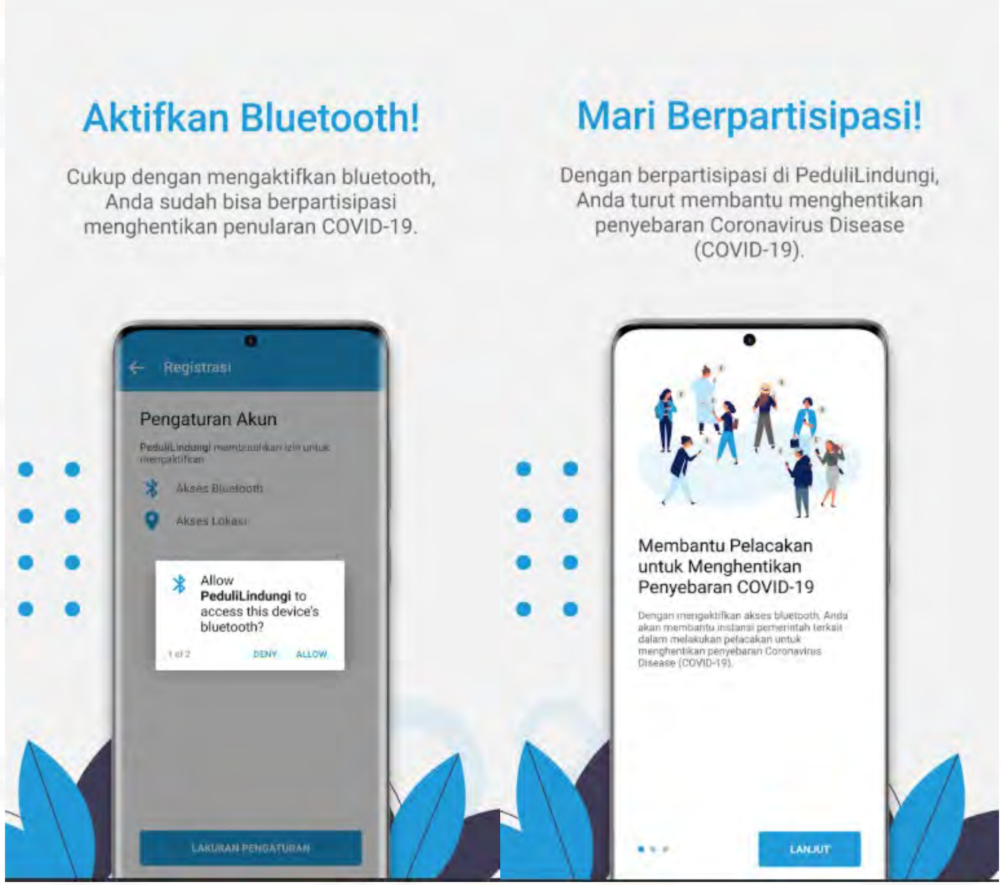
Nama Lengkap

Nomor Handphone

How PeduliLindungi works

The app will only give a notification if:

- The user is identified as being in a crowded area, i.e. is in the same place as several other users that have been actively using the app (based on zones).
- The user enters a certain zone:
  - **The red zone** is the area that has been recorded that someone is positively infected with Covid-19 or there is a patient under surveillance (PDP).
  - **Yellow zone** is an area that has been recorded that there are people being monitored (ODP).
  - **Green zone** is an area that has been recorded that there are no PDP, ODP, or infected covid-19 cases.
- The app also tracks users under self-quarantine status – if the user is out of the quarantine or isolation zone.



Aktifkan Bluetooth!

Cukup dengan mengaktifkan bluetooth, Anda sudah bisa berpartisipasi menghentikan penularan COVID-19.

Registrasi

Pengaturan Akun

PeduliLindungi membutuhkan izin untuk mengaktifkan

Akses Bluetooth

Akses Lokasi

Allow **PeduliLindungi** to access this device's bluetooth?

1 of 2 DENY ALLOW

LAKUKAN PENGATURAN

Mari Berpartisipasi!

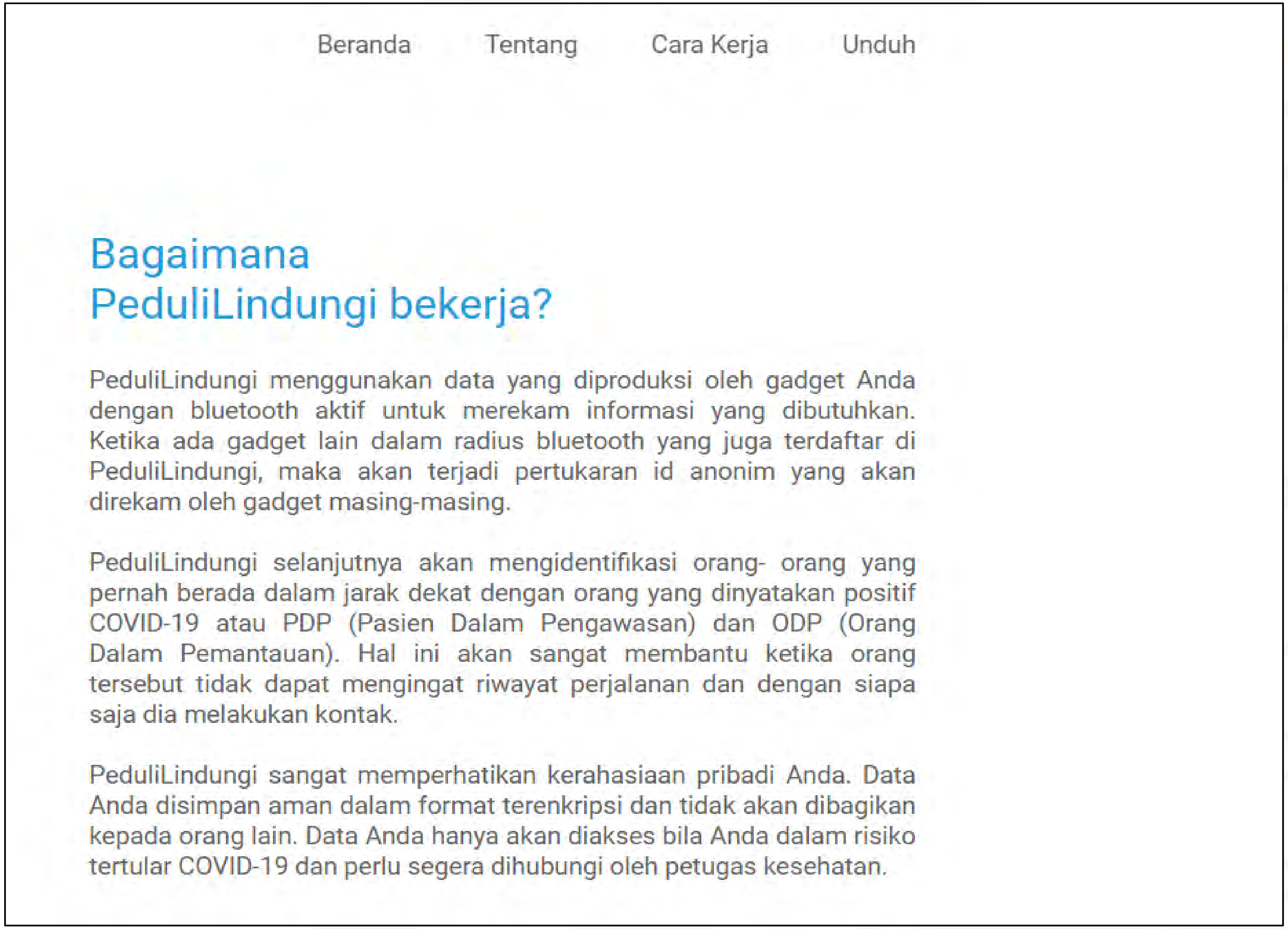
Dengan berpartisipasi di PeduliLindungi, Anda turut membantu menghentikan penyebaran Coronavirus Disease (COVID-19).

Membantu Pelacakan untuk Menghentikan Penyebaran COVID-19

Dengan mengaktifkan akses bluetooth, Anda akan membantu instansi pemerintah terkait dalam melakukan pelacakan untuk menghentikan penyebaran Coronavirus Disease (COVID-19).

LANJUT

Privacy Notice



Bagaimana PeduliLindungi bekerja?

PeduliLindungi menggunakan data yang diproduksi oleh gadget Anda dengan bluetooth aktif untuk merekam informasi yang dibutuhkan. Ketika ada gadget lain dalam radius bluetooth yang juga terdaftar di PeduliLindungi, maka akan terjadi pertukaran id anonim yang akan direkam oleh gadget masing-masing.

PeduliLindungi selanjutnya akan mengidentifikasi orang- orang yang pernah berada dalam jarak dekat dengan orang yang dinyatakan positif COVID-19 atau PDP (Pasien Dalam Pengawasan) dan ODP (Orang Dalam Pemantauan). Hal ini akan sangat membantu ketika orang tersebut tidak dapat mengingat riwayat perjalanan dan dengan siapa saja dia melakukan kontak.

PeduliLindungi sangat memperhatikan kerahasiaan pribadi Anda. Data Anda disimpan aman dalam format terenkripsi dan tidak akan dibagikan kepada orang lain. Data Anda hanya akan diakses bila Anda dalam risiko tertular COVID-19 dan perlu segera dihubungi oleh petugas kesehatan.

Privacy statement **does not clearly state how personal data is processed.** It just says:

- “PeduliLindungi respects the user’s privacy.
- The user data will be encrypted and not be disclosed to any other party.
- The user data can only be accessed if he/she is likely to have been infected with COVID-19 and require immediate medical attention,”
- No other explanation

However, once the app has been downloaded, under the **terms and conditions,** it will tell generally how the personal data is processed

Overview of Permissions Used

Dangerous permissions used in PeduliLindungi

Location	• precise location (GPS and network-based) • approximate location (network-based)
Photos/Media/ Files	• read the contents of your USB storage • modify or delete the contents of your USB storage
Camera	• take pictures and videos
Storage	• read the contents of your USB storage • modify or delete the contents of your USB storage

Overview of Permissions Used

Dangerous permissions used in PeduliLindungi

Normal	• receive data from Internet • full network access • prevent device from sleeping • run at startup • access Bluetooth settings • view network connections • pair with Bluetooth devices

Use of Permissions

Location

According to the privacy statement for the PeduliLindungi app:

- ‘PeduliLindungi is intended to conduct health surveillance… (It relies on concern and community participation **to share location data with each other** while travelling so that tracing of the contact history with sufferers of COVID-19 can be done).

- This is used to identify if users are in certain specific zones.
- The app asks for consent for location and Bluetooth permission.

Use of Permissions

Photos/Media/Files/Storage

- We can see that PeduliLindungi seeks permission to:
- modify or delete the contents of the USB storage in a user's mobile phone
- read the contents of a user's USB storage in their mobile phone

Justification: permissions are sought so that the app can store 'close proximity' information for the last 14 days. This means that the 'close proximity' information can be read if it becomes necessary to trace the user's contacts.

- The privacy notice indicates that the data will be deleted after COVID19 period ends.

Use of Permissions

Photos/Media/Files/Storage

The privacy statement in the PeduliLindungi app says that:

- ‘The user data will only be accessed if the user is deemed to be at risk of infection’.

- ‘It means that this data will be used solely for contact tracing of persons possibly exposed to COVID-19.’

- *However, it is unclear how user will share that data with the government if there is an infected case (i.e. no upload button)*

Use of Permissions

Camera

- PeduliLindungi seeks permission to:
- Take pictures and videos

Justification: In certain public space, certain information could be made available may require a QR code scan web site URL (which is not clearly stated in either the privacy statement or terms and conditions). This is only applicable to overseas visitors at the immigration gate and for those participating in rapid COVID19 tests.

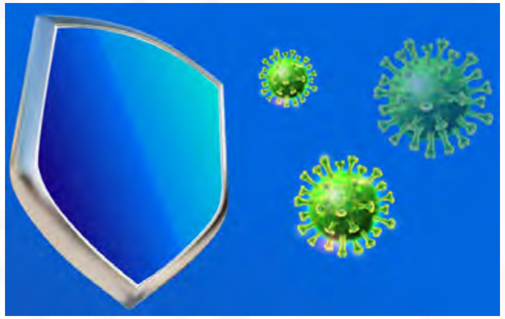
There may be considered excessive given that the objective of the apps is specifically for contact tracing purposes. (There are already other QR code apps that can be used)

	Indonesia
PRIVACY COMMUNICATIONS	PeduliLindungi
Apps with concerns regarding pre-installation privacy communications	**No Issue**
Apps with excessive permissions based on sweeper’s understanding of app’s functionality	**Yes**, there are excessive permissions requested within PeduliLindungi (as explained)
Apps with privacy communications not well tailored to small screen	**Yes,** it is not tailored to the small screen. Information provided cannot be read properly.

OVERALL PRIVACY MARKS	PeduliLindungi
0 = No privacy information, other than permissions	
1 = Privacy information not adequate; sweeper does not know how information will be collected, used and disclosed	
2 = Privacy information somewhat explains the app’s collection, use and disclosure of personal information; however, sweeper still had questions about certain permissions	Yes
3 = Privacy information clearly explains how app collects/uses/discloses personal information; sweeper is confident in his/her knowledge of app’s practices	

Bluezone Review

Ng Quan Cheng

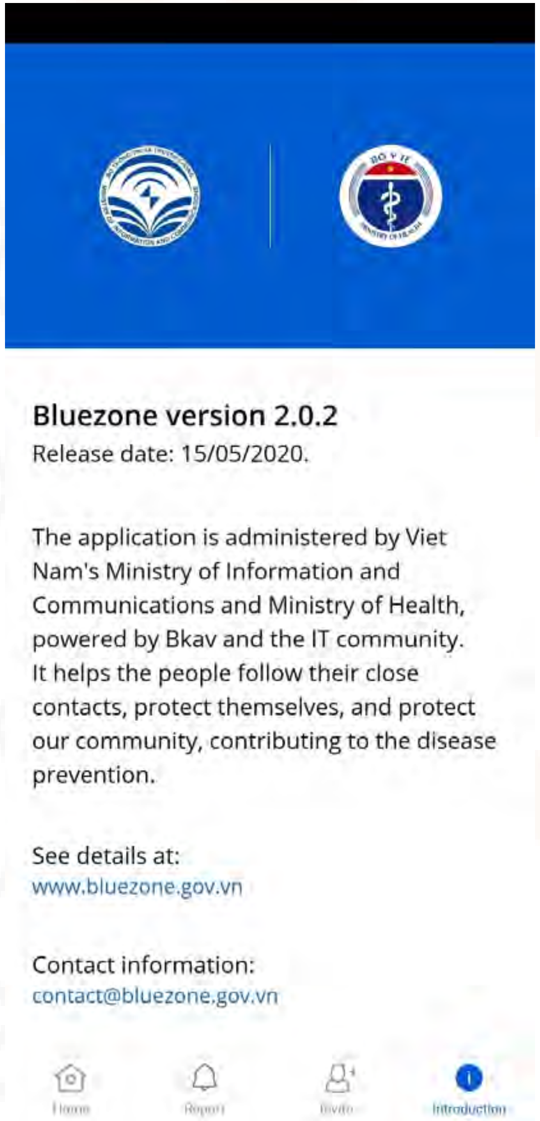


Photos taken from bluezone.gov.vn/bluezone.ai - Modified

Objectives of Bluezone

The objectives of the Bluezone app are to:

- 'protect' and 'bring life back to normal' against COVID-19 pandemic
- 'minimizing the spread of the virus to the community' by alerting if you had 'close contact' with people who are infected
- allow user to learn whether he/she had close contact with new case of infection or not simply by accessing the app



Bluezone version 2.0.2

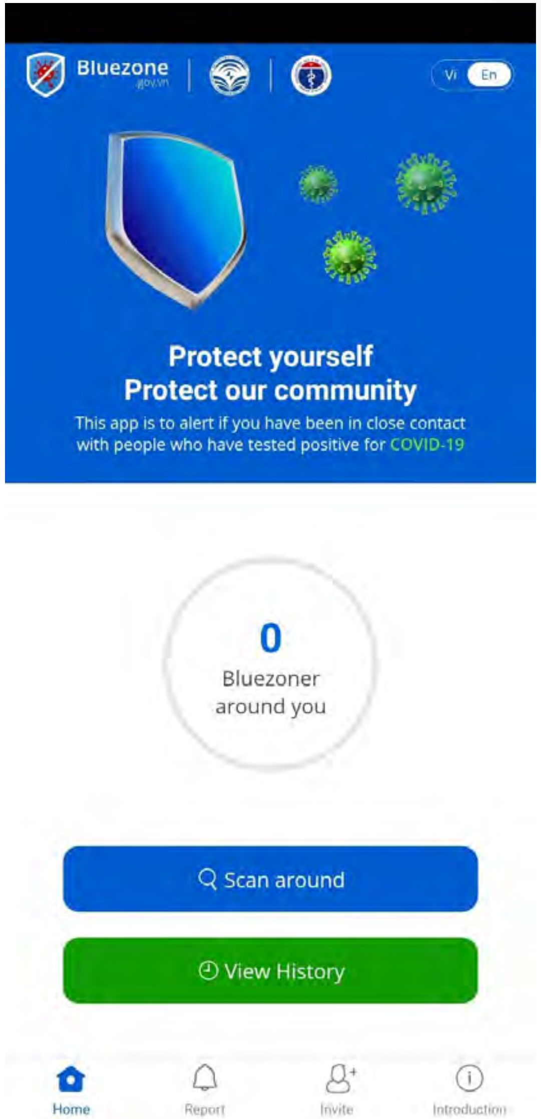
Release date: 15/05/2020.

The application is administered by Viet Nam's Ministry of Information and Communications and Ministry of Health, powered by Bkav and the IT community. It helps the people follow their close contacts, protect themselves, and protect our community, contributing to the disease prevention.

See details at:
www.bluezone.gov.vn

Contact information:
contact@bluezone.gov.vn

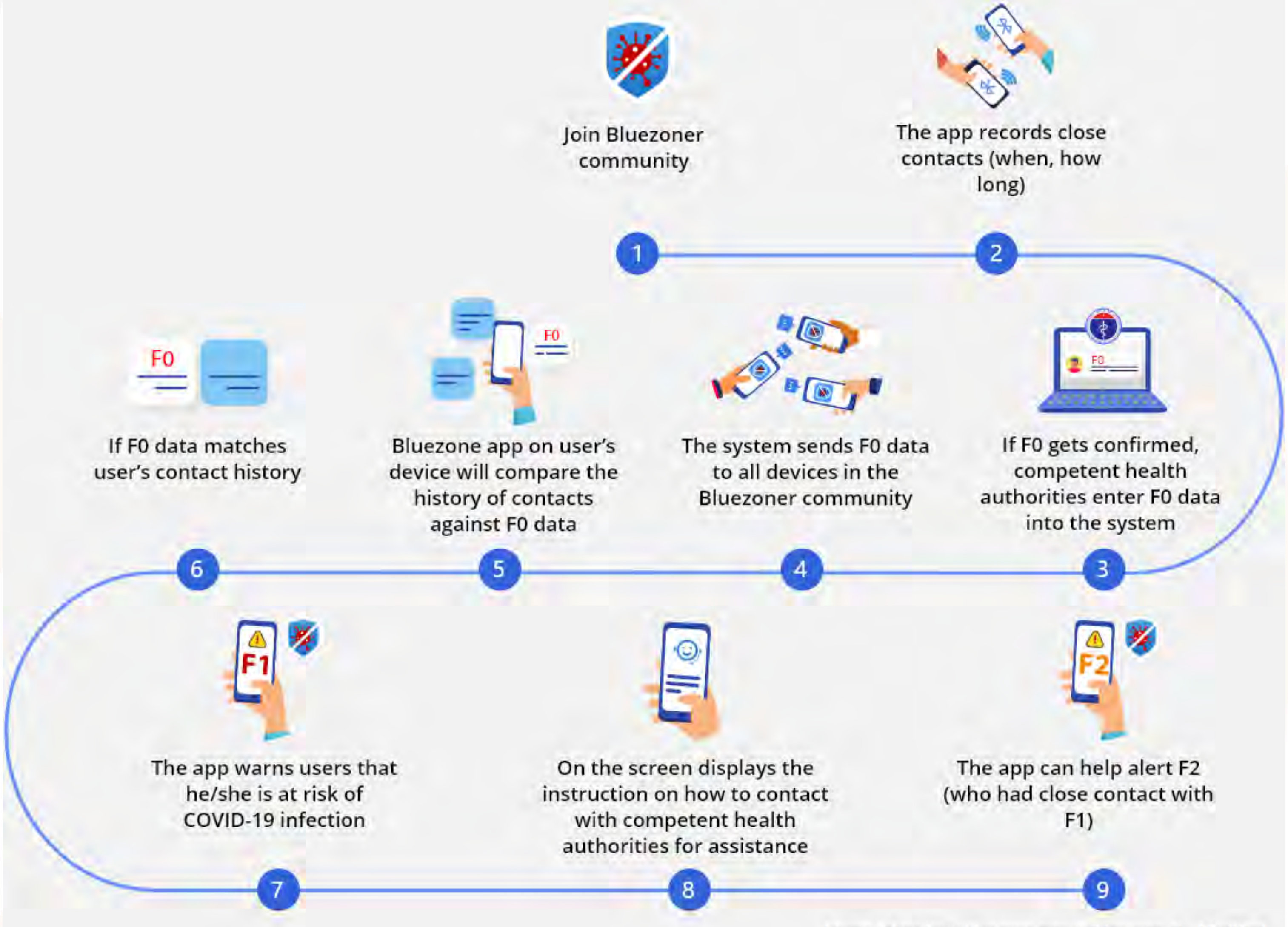
How Bluezone works



Protect yourself
Protect our community

This app is to alert if you have been in close contact with people who have tested positive for COVID-19

0
Bluezoner
around you

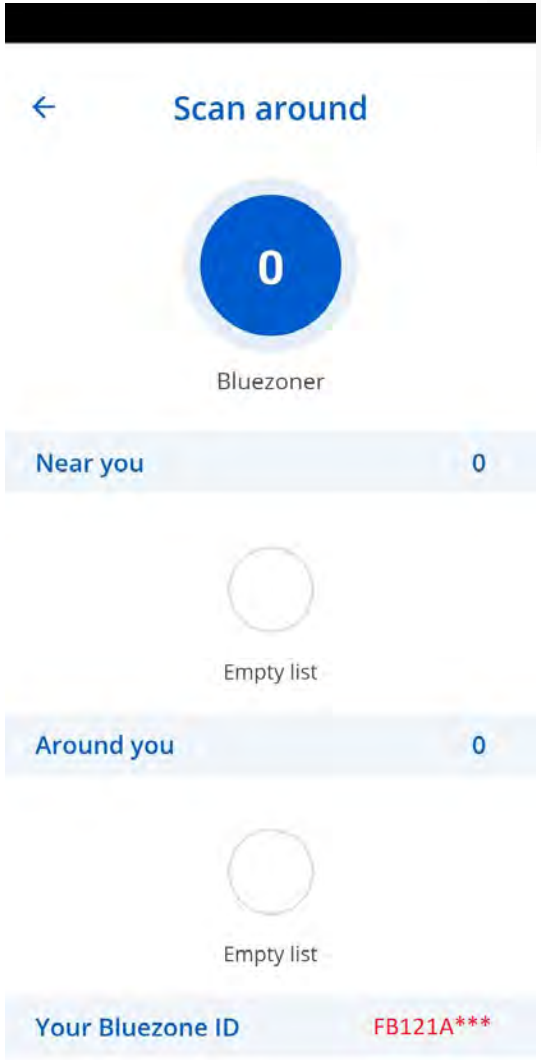


1. Join Bluezoner community
2. The app records close contacts (when, how long)
3. If F0 gets confirmed, competent health authorities enter F0 data into the system
4. The system sends F0 data to all devices in the Bluezoner community
5. Bluezone app on user's device will compare the history of contacts against F0 data
6. If F0 data matches user's contact history
7. The app warns users that he/she is at risk of COVID-19 infection
8. On the screen displays the instruction on how to contact with competent health authorities for assistance
9. The app can help alert F2 (who had close contact with F1)

Image taken from bluezone.gov.vn/bluezone.ai - Modified

How Bluezone works

Initiating Manual Scan



Scan around

0

Bluezoner

Near you 0

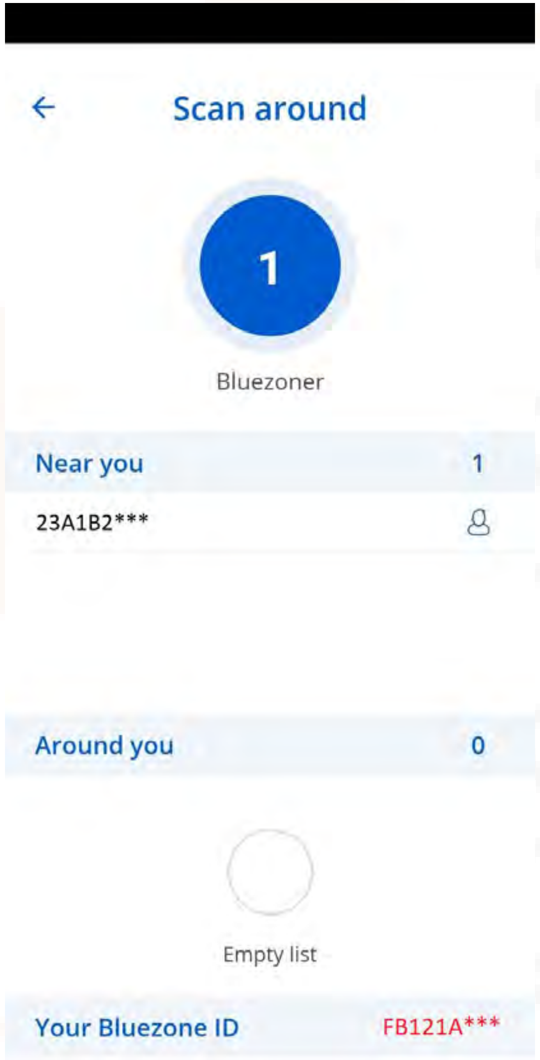
Empty list

Around you 0

Empty list

Your Bluezone ID FB121A***

Nearby Bluezone User



Scan around

1

Bluezoner

Near you 1

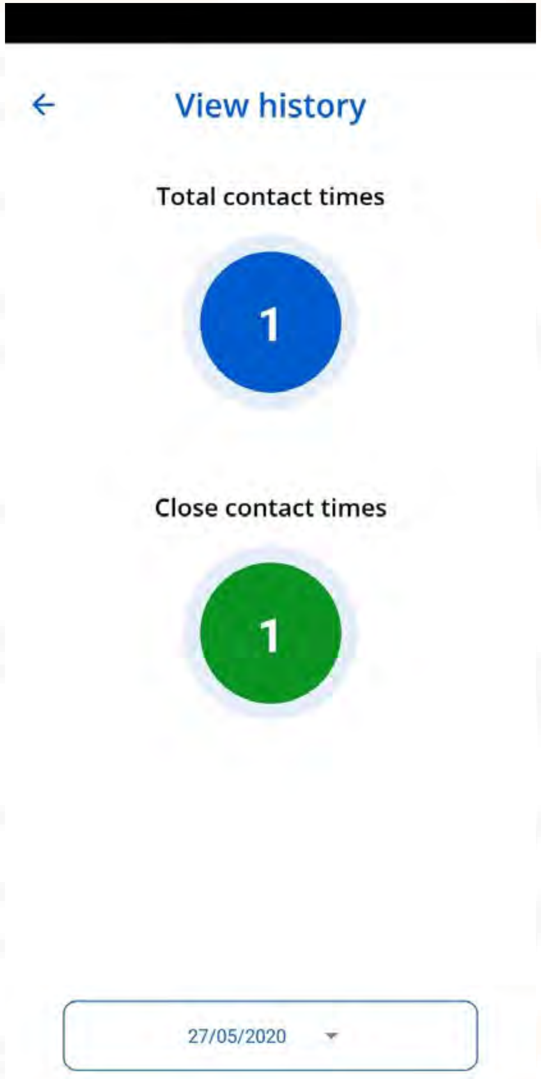
23A1B2***

Around you 0

Empty list

Your Bluezone ID FB121A***

History View



View history

Total contact times

1

Close contact times

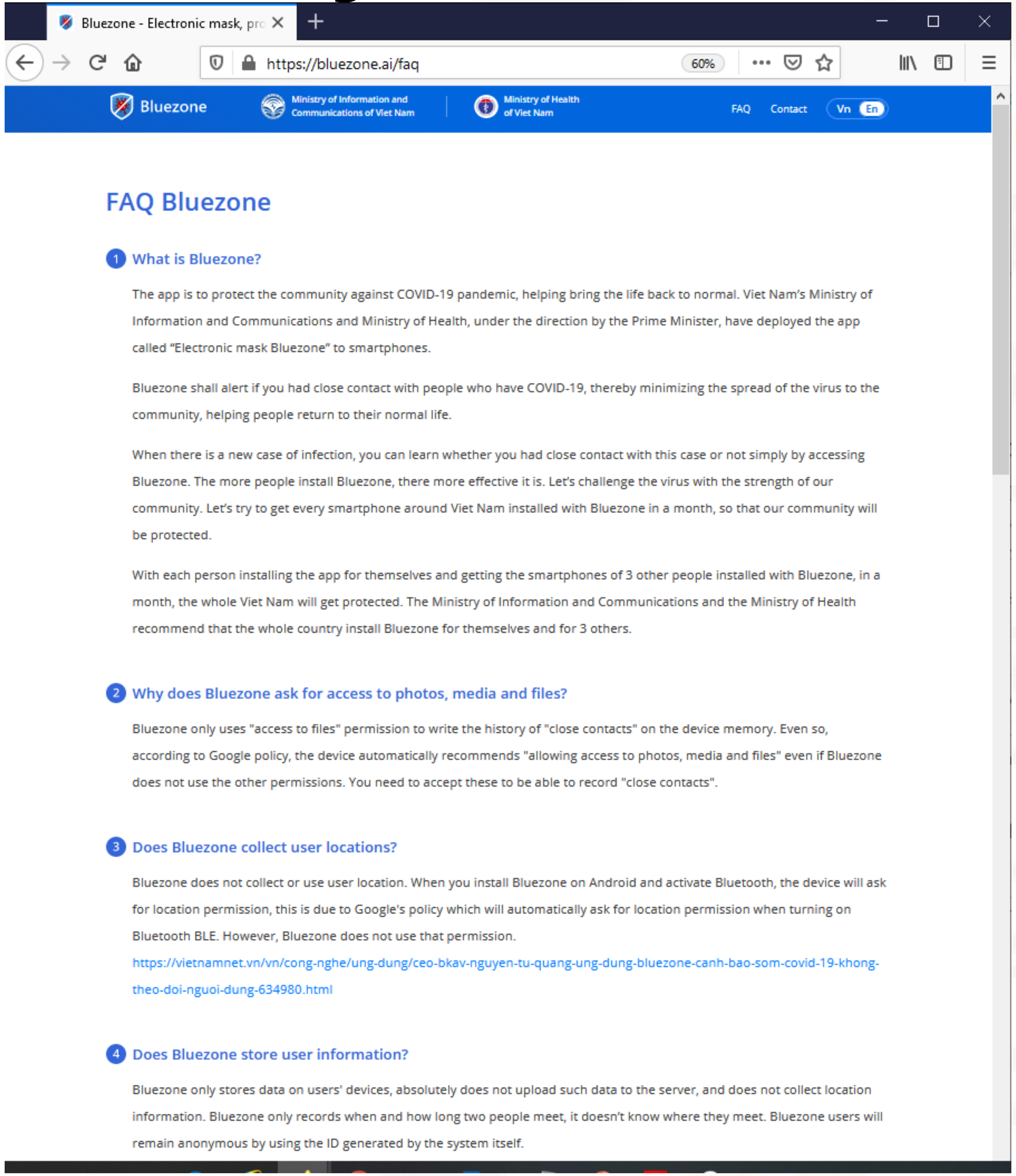
1

27/05/2020

User has the option to scan who else might be using the same app around them

While this may be intended to encourage participation, it might cause concerns for users worried about their own privacy.

Privacy Notice


Bluezone - Electronic mask, pro
https://bluezone.ai/faq
60%
Bluezone
Ministry of Information and Communications of Viet Nam
Ministry of Health of Viet Nam
FAQ
Contact
Vn
En

FAQ Bluezone

1 What is Bluezone?

The app is to protect the community against COVID-19 pandemic, helping bring the life back to normal. Viet Nam's Ministry of Information and Communications and Ministry of Health, under the direction by the Prime Minister, have deployed the app called "Electronic mask Bluezone" to smartphones.

Bluezone shall alert if you had close contact with people who have COVID-19, thereby minimizing the spread of the virus to the community, helping people return to their normal life.

When there is a new case of infection, you can learn whether you had close contact with this case or not simply by accessing Bluezone. The more people install Bluezone, there more effective it is. Let's challenge the virus with the strength of our community. Let's try to get every smartphone around Viet Nam installed with Bluezone in a month, so that our community will be protected.

With each person installing the app for themselves and getting the smartphones of 3 other people installed with Bluezone, in a month, the whole Viet Nam will get protected. The Ministry of Information and Communications and the Ministry of Health recommend that the whole country install Bluezone for themselves and for 3 others.

2 Why does Bluezone ask for access to photos, media and files?

Bluezone only uses "access to files" permission to write the history of "close contacts" on the device memory. Even so, according to Google policy, the device automatically recommends "allowing access to photos, media and files" even if Bluezone does not use the other permissions. You need to accept these to be able to record "close contacts".

3 Does Bluezone collect user locations?

Bluezone does not collect or use user location. When you install Bluezone on Android and activate Bluetooth, the device will ask for location permission, this is due to Google's policy which will automatically ask for location permission when turning on Bluetooth BLE. However, Bluezone does not use that permission. https://vietnamnet.vn/vn/cong-nghe/ung-dung/ceo-bkav-nguyen-tu-quang-ung-dung-bluezone-canh-bao-som-covid-19-khong-theo-doi-nguoi-dung-634980.html

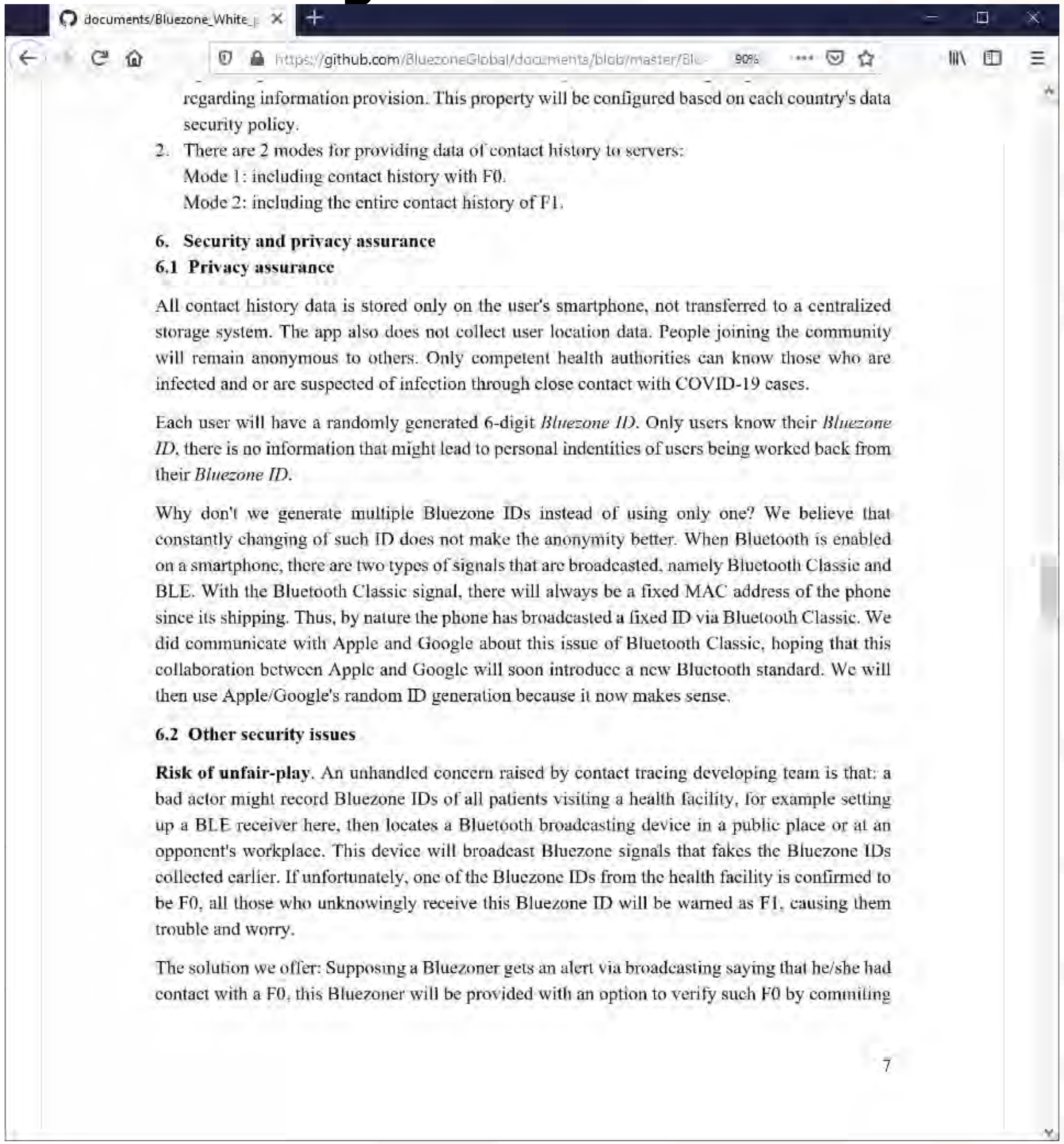
4 Does Bluezone store user information?

Bluezone only stores data on users' devices, absolutely does not upload such data to the server, and does not collect location information. Bluezone only records when and how long two people meet, it doesn't know where they meet. Bluezone users will remain anonymous by using the ID generated by the system itself.

Bluezone App

- There is no privacy notice.
- However, FAQ is used to address some privacy concerns
    - Permissions required during Installation
    - What does it, or does it not, collect
    - Why it is necessary
    - Did **not** specify how long the data is stored

Privacy Notice


documents/Bluezone_White_
https://github.com/BluezoneGlobal/documents/blob/master/Bl
90%

regarding information provision. This property will be configured based on each country's data security policy.

2. There are 2 modes for providing data of contact history to servers:
   Mode 1: including contact history with F0.
   Mode 2: including the entire contact history of F1.

6. Security and privacy assurance

6.1 Privacy assurance

All contact history data is stored only on the user's smartphone, not transferred to a centralized storage system. The app also does not collect user location data. People joining the community will remain anonymous to others. Only competent health authorities can know those who are infected and or are suspected of infection through close contact with COVID-19 cases.

Each user will have a randomly generated 6-digit *Bluezone ID*. Only users know their *Bluezone ID*, there is no information that might lead to personal indentities of users being worked back from their *Bluezone ID*.

Why don't we generate multiple Bluezone IDs instead of using only one? We believe that constantly changing of such ID does not make the anonymity better. When Bluetooth is enabled on a smartphone, there are two types of signals that are broadcasted, namely Bluetooth Classic and BLE. With the Bluetooth Classic signal, there will always be a fixed MAC address of the phone since its shipping. Thus, by nature the phone has broadcasted a fixed ID via Bluetooth Classic. We did communicate with Apple and Google about this issue of Bluetooth Classic, hoping that this collaboration between Apple and Google will soon introduce a new Bluetooth standard. We will then use Apple/Google's random ID generation because it now makes sense.

6.2 Other security issues

Risk of unfair-play. An unhandled concern raised by contact tracing developing team is that: a bad actor might record Bluezone IDs of all patients visiting a health facility, for example setting up a BLE receiver here, then locates a Bluetooth broadcasting device in a public place or at an opponent's workplace. This device will broadcast Bluezone signals that fakes the Bluezone IDs collected earlier. If unfortunately, one of the Bluezone IDs from the health facility is confirmed to be F0, all those who unknowingly receive this Bluezone ID will be warned as F1, causing them trouble and worry.

The solution we offer: Supposing a Bluezoner gets an alert via broadcasting saying that he/she had contact with a F0, this Bluezoner will be provided with an option to verify such F0 by commiting

7

Bluezone App

- Detailed Data Privacy and functions of the app are found in whitepapers for developers instead.

URL - https://bit.ly/BluezoneWPEN

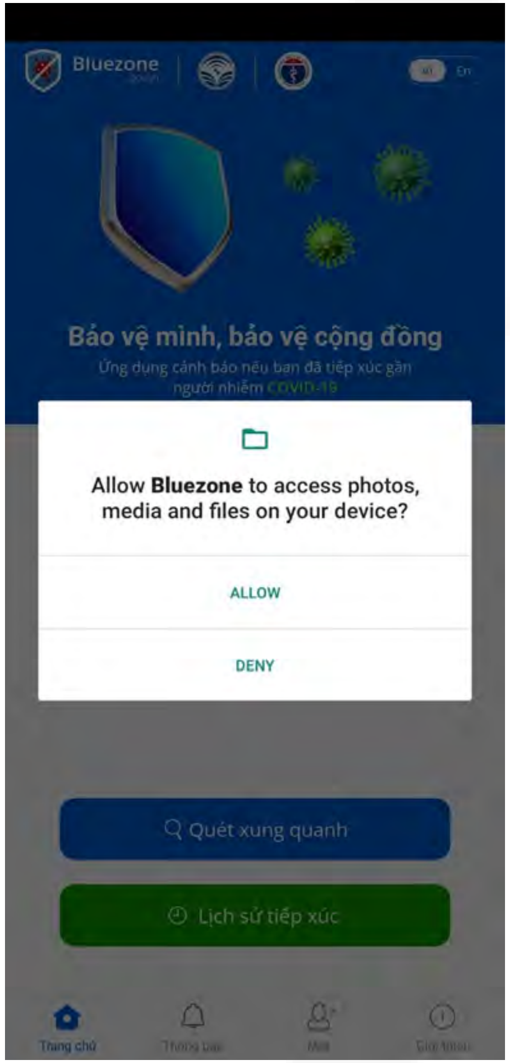
Overview of Permissions Used

Dangerous permissions used in Bluezone

Photos/Media/ Files	• read the contents of your USB storage • modify or delete the contents of your USB storage
Storage	• read the contents of your USB storage • modify or delete the contents of your USB storage
Location	• approximate location (network-based) • precise location (GPS and network-based)
Normal	• receive data from Internet • access Bluetooth settings • full network access • prevent device from sleeping • view network connections • pair with Bluetooth devices • run at startup

Use of Permissions

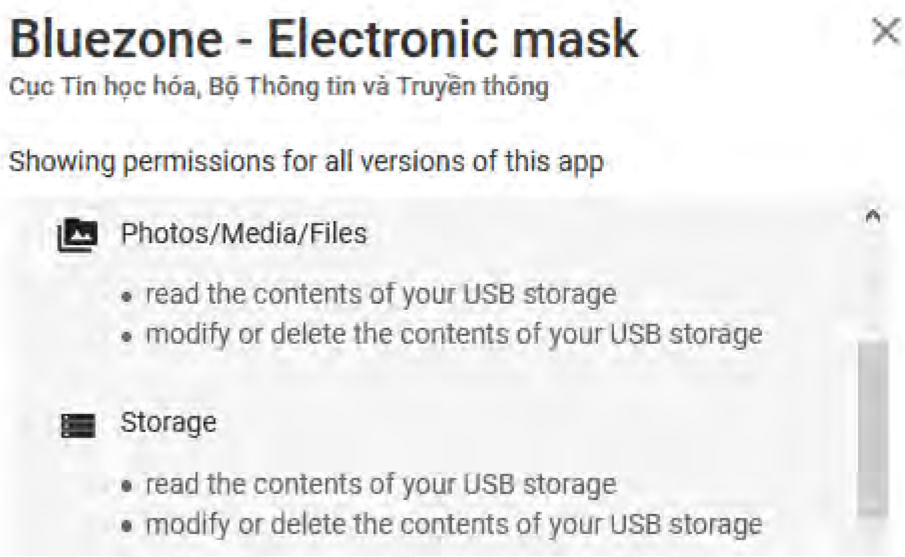
Photos/Media/Files/Storage



Bảo vệ mình, bảo vệ cộng đồng

Ứng dụng cảnh báo nếu bạn đã tiếp xúc gần người nhiễm COVID-19

Allow **Bluezone** to access photos, media and files on your device?



Bluezone - Electronic mask

Cục Tin học hóa, Bộ Thông tin và Truyền thông

Showing permissions for all versions of this app

Photos/Media/Files

- read the contents of your USB storage
- modify or delete the contents of your USB storage

Storage

- read the contents of your USB storage
- modify or delete the contents of your USB storage

It is unclear how a user will share that data with the government if there is an infected case (i.e. no upload button)

Justification:

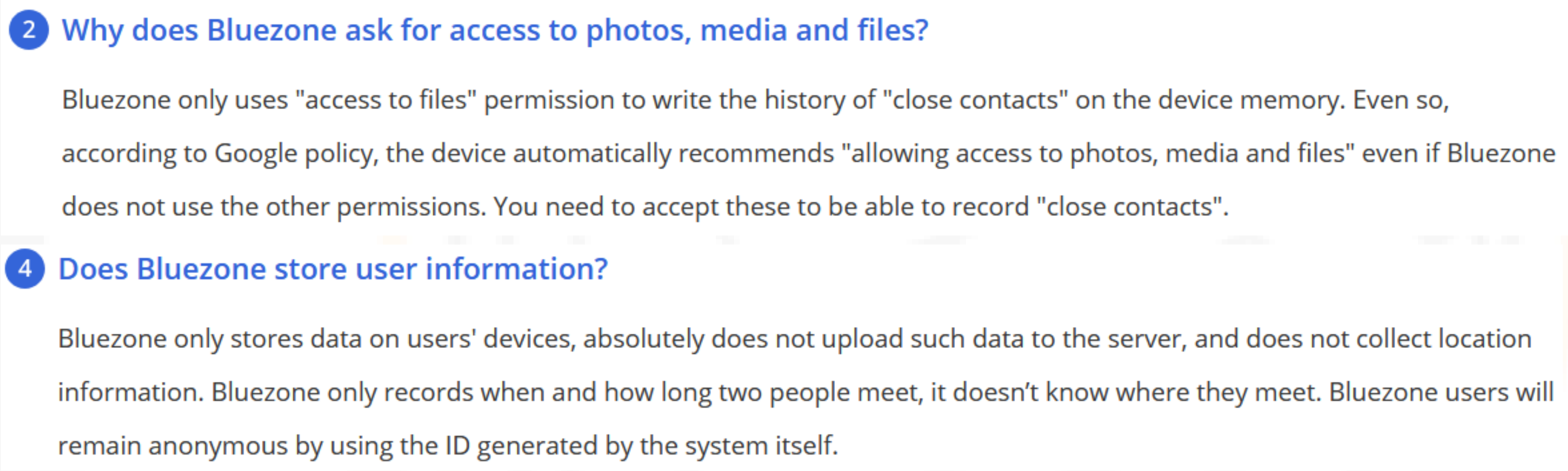
Permissions are sought so that the app can store ‘close contact’ information. This means that history of ‘close contact’ information can be extracted by authorities for contact tracing purposes.

Use of Permissions

Photos/Media/Files/Storage

Mentioned in Bluezone FAQ:

- Explained why the permission is requested
- What and how the data is collected
- Did **not** mention retention period of data stored



2 Why does Bluezone ask for access to photos, media and files?

Bluezone only uses "access to files" permission to write the history of "close contacts" on the device memory. Even so, according to Google policy, the device automatically recommends "allowing access to photos, media and files" even if Bluezone does not use the other permissions. You need to accept these to be able to record "close contacts".

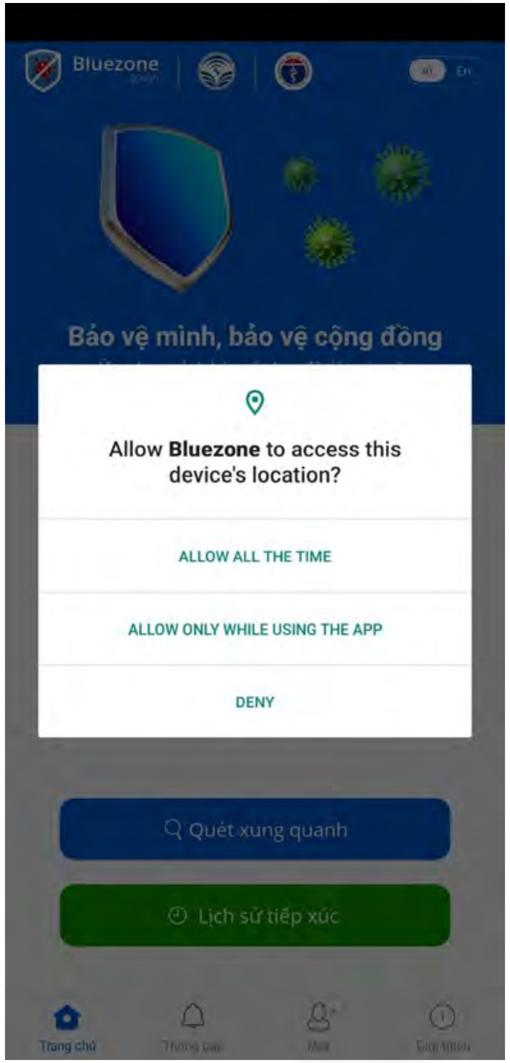
4 Does Bluezone store user information?

Bluezone only stores data on users' devices, absolutely does not upload such data to the server, and does not collect location information. Bluezone only records when and how long two people meet, it doesn't know where they meet. Bluezone users will remain anonymous by using the ID generated by the system itself.

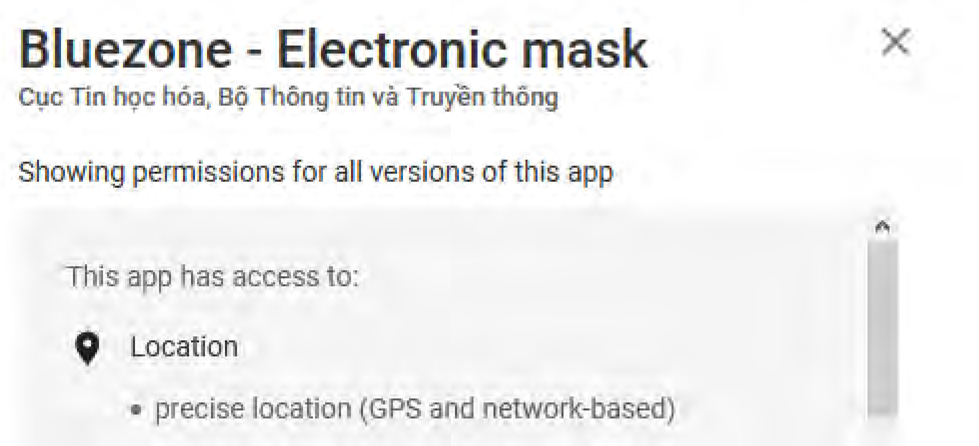
Extracted information from bluezone.ai

Use of Permissions

Location



Allow **Bluezone** to access this device's location?



Bluezone - Electronic mask

Cục Tin học hóa, Bộ Thông tin và Truyền thông

Showing permissions for all versions of this app

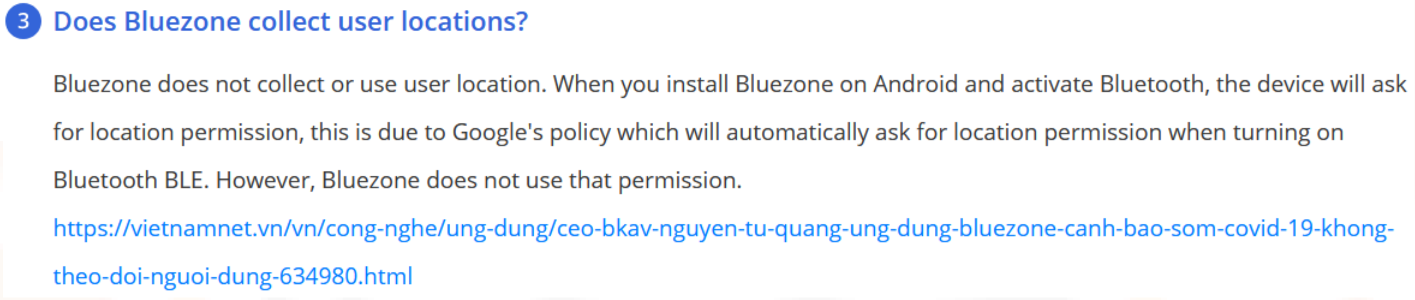
This app has access to:

Location

- precise location (GPS and network-based)

Mentioned in Bluezone FAQ:

- Explained why the permission is requested
- App does not collect or use user location



3 Does Bluezone collect user locations?

Bluezone does not collect or use user location. When you install Bluezone on Android and activate Bluetooth, the device will ask for location permission, this is due to Google's policy which will automatically ask for location permission when turning on Bluetooth BLE. However, Bluezone does not use that permission.

https://vietnamnet.vn/vn/cong-nghe/ung-dung/ceo-bkav-nguyen-tu-quang-ung-dung-bluezone-canh-bao-som-covid-19-khong-theo-doi-nguoi-dung-634980.html

	Vietnam
PRIVACY COMMUNICATIONS	Bluezone
Apps with concerns regarding pre-installation privacy communications	**Yes** No reference to mobile permissions being used
Apps with excessive permissions based on sweeper’s understanding of app’s functionality	**No Issues**
Apps with privacy communications not well tailored to small screen	**No Issues**

OVERALL PRIVACY MARKS	Bluezone
0 = No privacy information, other than permissions	
1 = Privacy information not adequate; sweeper does not know how information will be collected, used and disclosed	
2 = Privacy information somewhat explains the app’s collection, use and disclosure of personal information; however, sweeper still had questions about certain permissions	**YES.**
3 = Privacy information clearly explains how app collects/uses/discloses personal information; sweeper is confident in his/her knowledge of app’s practices	

Mor Chana Review

Loke Qian Li (FIP, CIPP/A, CIPM, GRCP)

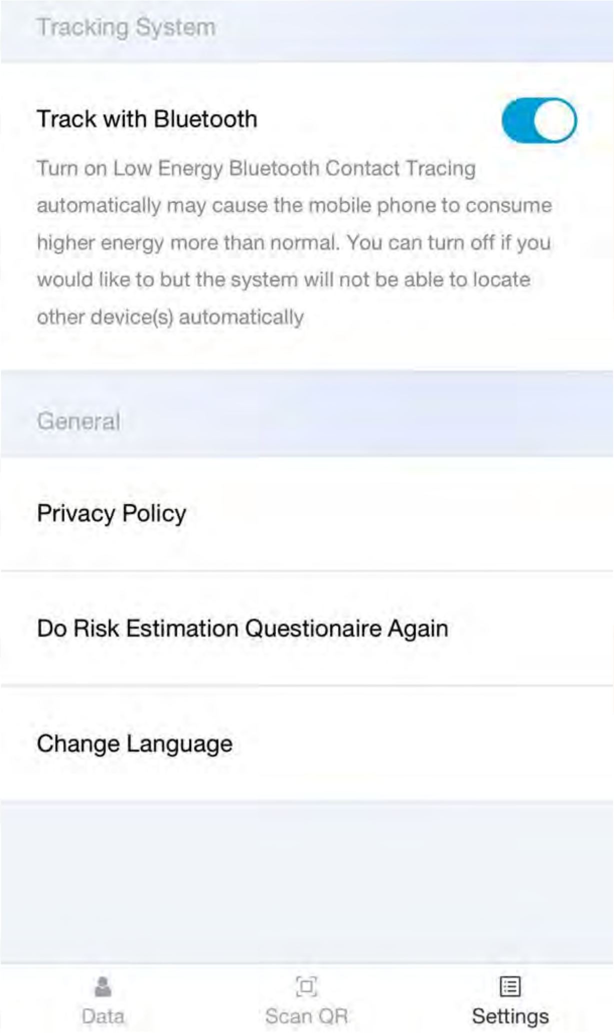
Sarah Wang Han (PhD candidate, LLM,LLB)

Objectives of Mor Chana

The objectives of the Mor Chana app are to:

- allow users to have self-observation to assess their coronavirus infection risk
- provide an infection alert and essential information necessary to screen infected or at-risk persons
- assist health authorities in tracking users in close contact with infected people and prevent transmission among healthcare workers*.

Source: Bangkok Post



Tracking System

Track with Bluetooth

Turn on Low Energy Bluetooth Contact Tracing automatically may cause the mobile phone to consume higher energy more than normal. You can turn off if you would like to but the system will not be able to locate other device(s) automatically

General

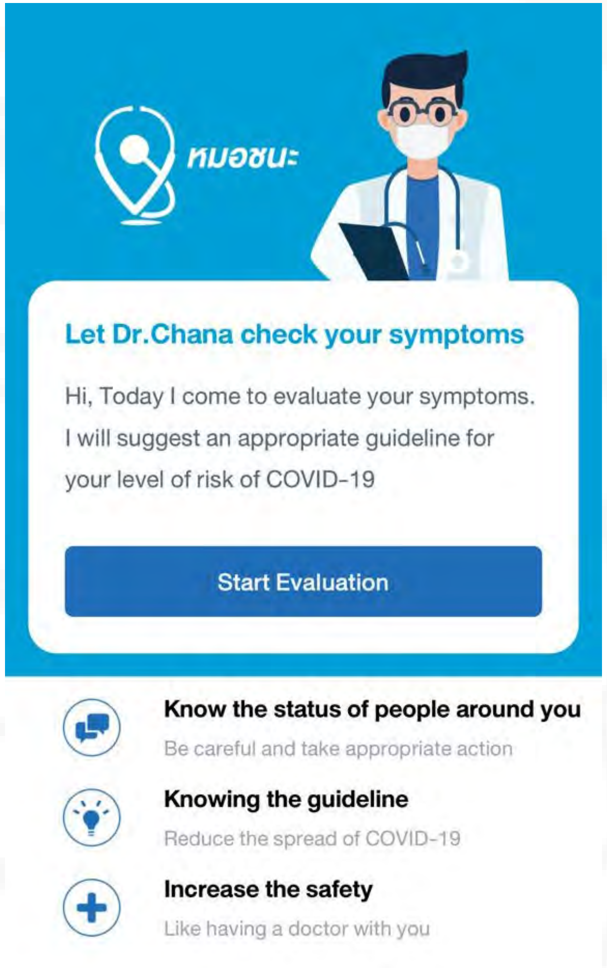
Privacy Policy

Do Risk Estimation Questionaire Again

Change Language

How Mor Chana works

- User downloads the app and registers.
- Upon registration, user is asked to take a photo of himself, user can voluntarily provide a phone number. If a phone number is provided, a healthcare professional may contact the user.
- The user is required to complete four self-assessment questions to determine the risk of being infected with the coronavirus.
- The result is then classified into four levels of risk indicated by four different colours.
- The app also assigns a QR code indicating the risk level of a user.



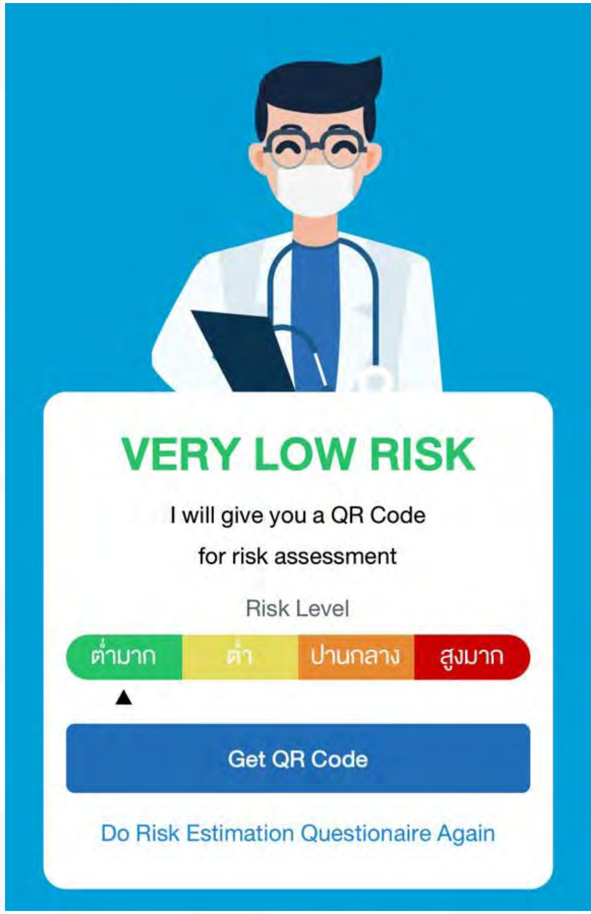
Let Dr.Chana check your symptoms

Hi, Today I come to evaluate your symptoms. I will suggest an appropriate guideline for your level of risk of COVID-19

Know the status of people around you
Be careful and take appropriate action

Knowing the guideline
Reduce the spread of COVID-19

Increase the safety
Like having a doctor with you



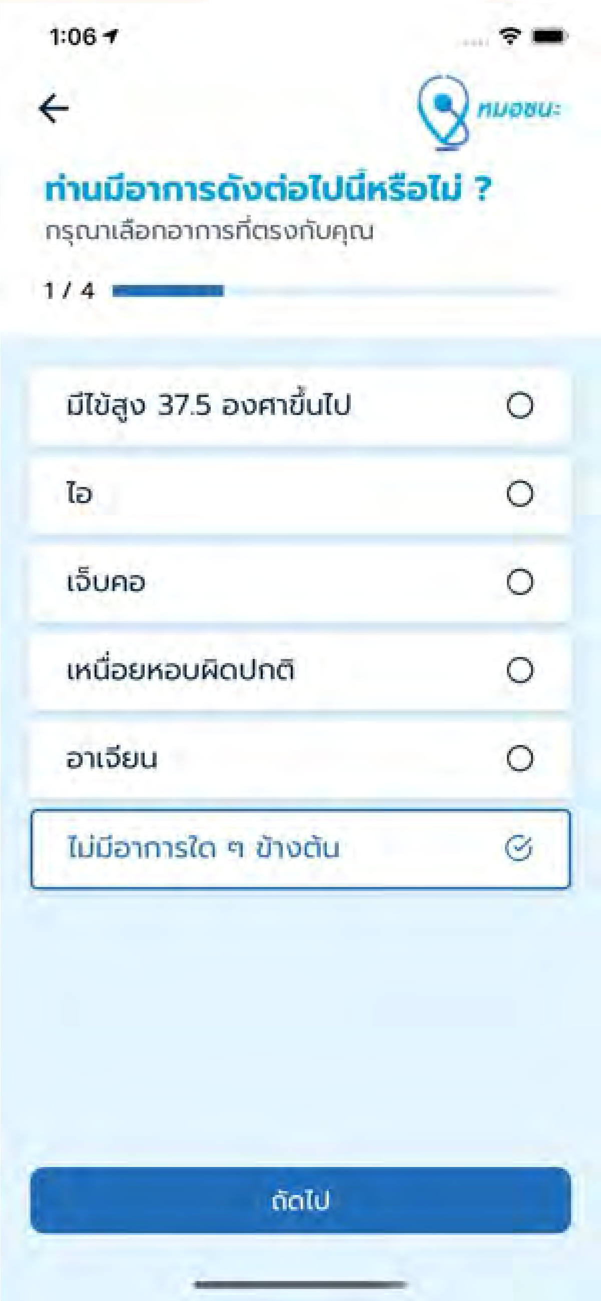
VERY LOW RISK

I will give you a QR Code
for risk assessment

Risk Level

How Mor Chana works

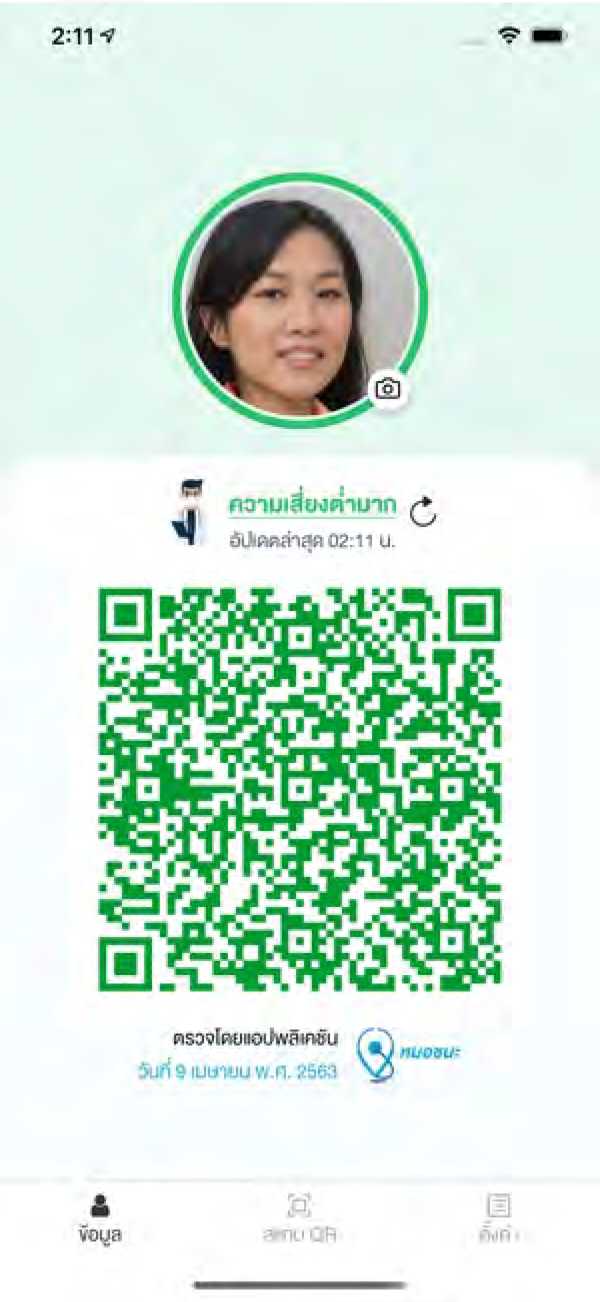
- When the data size reaches a critical mass for data analytics to be performed, the app may adjust the risk level for a user by changing the colour.
- User may be asked by the authorities to share their records stored in their phones as part of contact tracing investigations.
- The app uses GPS and Bluetooth to track contact history.
- User can use the app to identify locations or areas of potential risks.



ท่านมีอาการดังต่อไปนี้หรือไม่ ?

กรุณาเลือกอาการที่ตรงกับคุณ

- มีไข้สูง 37.5 องศาขึ้นไป ○
- ไอ ○
- เจ็บคอ ○
- เหนื่อยหอบผิดปกติ ○
- อาเจียน ○
- ไม่มีอาการใด ๆ ข้างต้น ✓



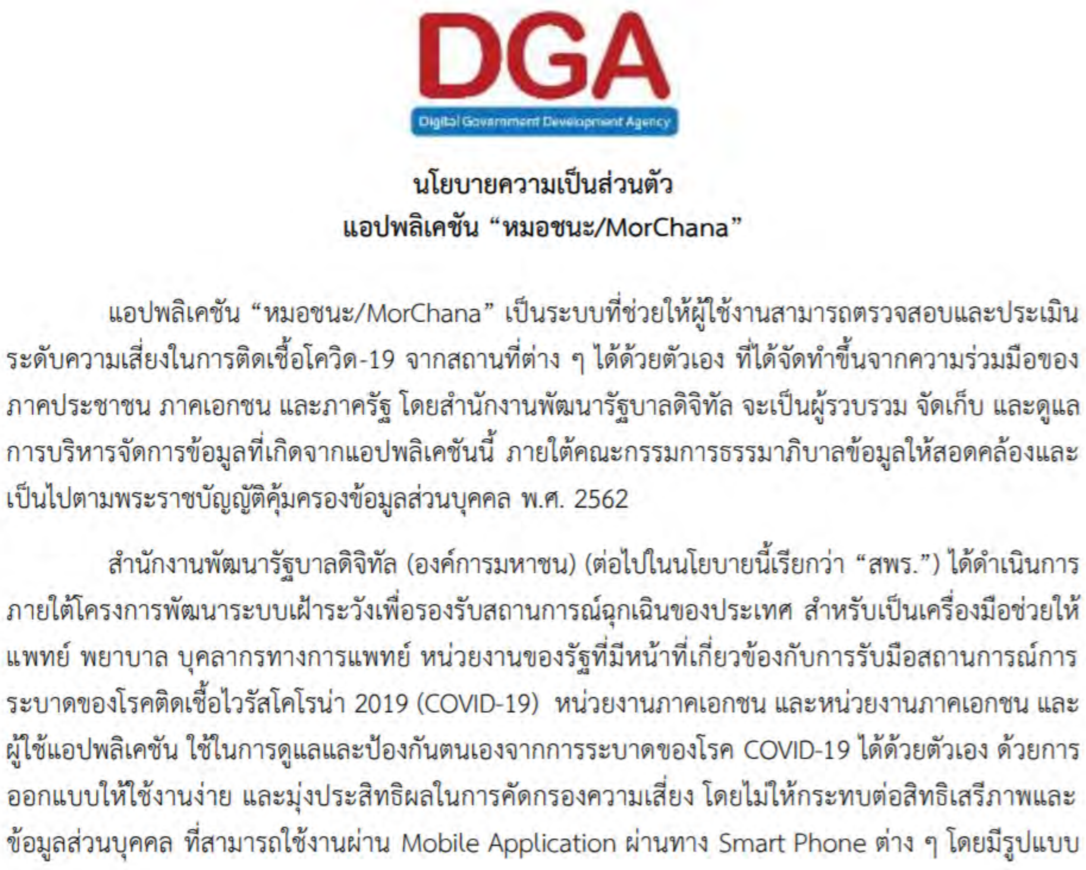
ความเสี่ยงต่ำมาก

อัปเดตล่าสุด 02:11 น.

ตรวจโดยแอปพลิเคชัน หมอชนะ

วันที่ 9 เมษายน พ.ศ. 2563

Privacy Notice



DGA

Digital Government Development Agency

นโยบายความเป็นส่วนตัว
แอปพลิเคชัน “หมอชนะ/MorChana”

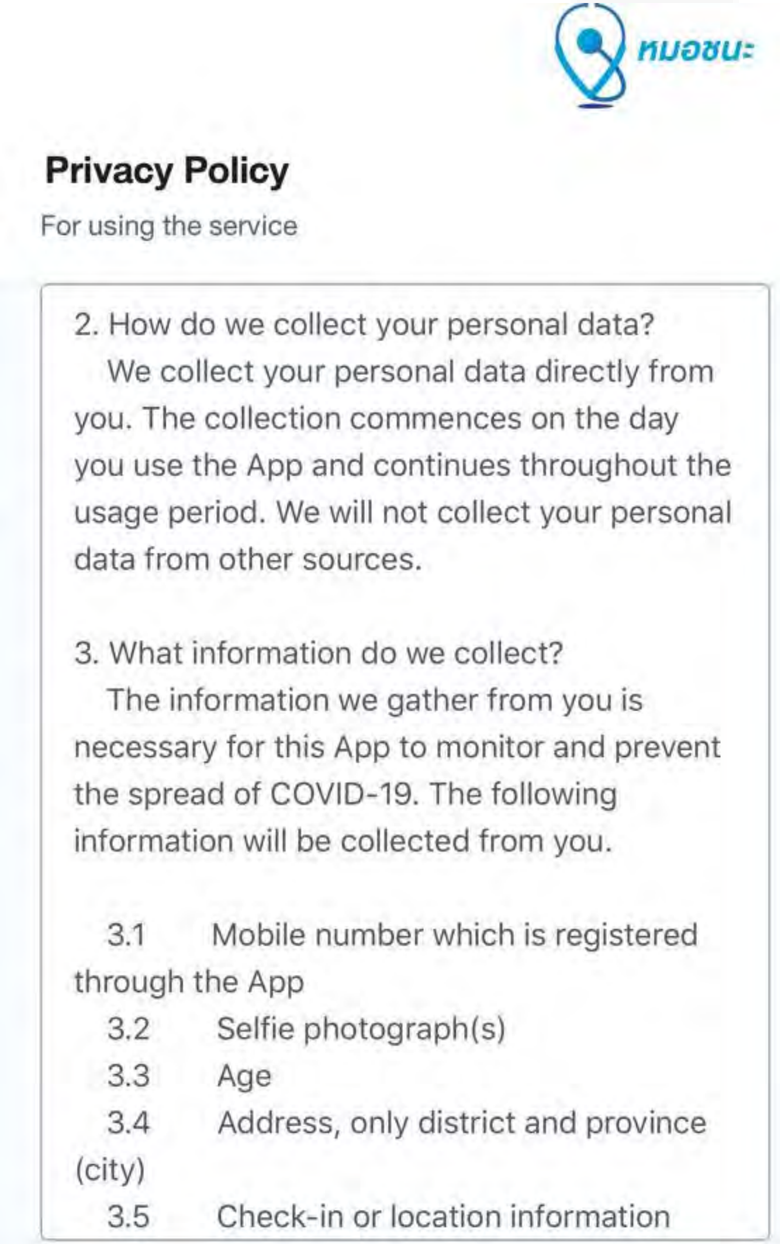
แอปพลิเคชัน “หมอชนะ/MorChana” เป็นระบบที่ช่วยให้ผู้ใช้งานสามารถตรวจสอบและประเมินระดับความเสี่ยงในการติดเชื้อโควิด-19 จากสถานที่ต่าง ๆ ได้ด้วยตัวเอง ที่ได้จัดทำขึ้นจากความร่วมมือของภาคประชาชน ภาคเอกชน และภาครัฐ โดยสำนักงานพัฒนารัฐบาลดิจิทัล จะเป็นผู้รวบรวม จัดเก็บ และดูแลการบริหารจัดการข้อมูลที่เกิดจากแอปพลิเคชันนี้ ภายใต้คณะกรรมการธรรมาภิบาลข้อมูลให้สอดคล้องและเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (ต่อไปในนโยบายนี้เรียกว่า “สพร.”) ได้ดำเนินการภายใต้โครงการพัฒนาระบบเฝ้าระวังเพื่อรองรับสถานการณ์ฉุกเฉินของประเทศ สำหรับเป็นเครื่องมือช่วยให้แพทย์ พยาบาล บุคลากรทางการแพทย์ หน่วยงานของรัฐที่มีหน้าที่เกี่ยวข้องกับการรับมือสถานการณ์การระบาดของโรคติดเชื้อไวรัสโคโรน่า 2019 (COVID-19) หน่วยงานภาคเอกชน และหน่วยงานภาคเอกชน และผู้ใช้แอปพลิเคชัน ใช้ในการดูแลและป้องกันตนเองจากการระบาดของโรค COVID-19 ได้ด้วยตัวเอง ด้วยการออกแบบให้ใช้งานง่าย และมุ่งประสิทธิผลในการคัดกรองความเสี่ยง โดยไม่ให้กระทบต่อสิทธิเสรีภาพและข้อมูลส่วนบุคคล ที่สามารถใช้งานผ่าน Mobile Application ผ่านทาง Smart Phone ต่าง ๆ โดยมีรูปแบบ

Source: Digital Government Development Agency (DGA)

- Detailed Privacy Statement for MorChana app available on DGA website.
- The privacy statement available via the app on PlayStore/App Store is directed to the general DGA privacy statement.
- The DGA-specific privacy statement is available via the MorChana page on the DGA website.
- It is only available in Thai.
- The privacy statement is displayed upon starting the app for the first time.

Privacy Notice



หมอชนะ

Privacy Policy

For using the service

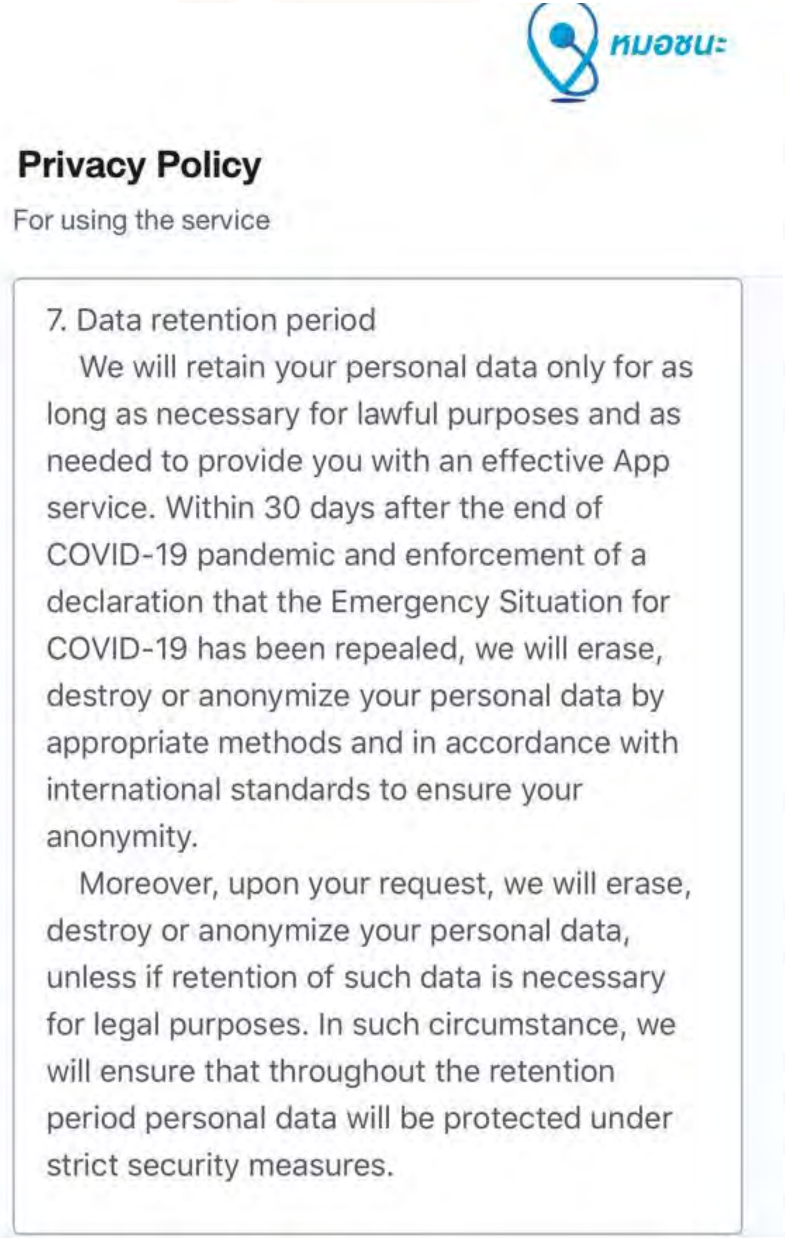
2. How do we collect your personal data?

We collect your personal data directly from you. The collection commences on the day you use the App and continues throughout the usage period. We will not collect your personal data from other sources.

3. What information do we collect?

The information we gather from you is necessary for this App to monitor and prevent the spread of COVID-19. The following information will be collected from you.

3.1 Mobile number which is registered through the App
3.2 Selfie photograph(s)
3.3 Age
3.4 Address, only district and province (city)
3.5 Check-in or location information



หมอชนะ

Privacy Policy

For using the service

7. Data retention period

We will retain your personal data only for as long as necessary for lawful purposes and as needed to provide you with an effective App service. Within 30 days after the end of COVID-19 pandemic and enforcement of a declaration that the Emergency Situation for COVID-19 has been repealed, we will erase, destroy or anonymize your personal data by appropriate methods and in accordance with international standards to ensure your anonymity.

Moreover, upon your request, we will erase, destroy or anonymize your personal data, unless if retention of such data is necessary for legal purposes. In such circumstance, we will ensure that throughout the retention period personal data will be protected under strict security measures.

- Privacy statement clearly states how personal data is processed and what personal data is being collected.
- Addresses concerns about retention period: “Within 30 days after the end of COVID-19 pandemic…, we will erase, destroy or anonymize your personal data…”.
- Allows data subject to request for deletion on reasonable grounds.

Overview of Permissions Used

Dangerous permissions used in Mor Chana

Photos/Media/ File Storage	• read the contents of your USB storage • modify or delete the contents of your USB storage
Wi-Fi Connection Camera	• View Wi-Fi connections • To take pictures and videos
Location	• approximate location (network-based) • precise location (GPS and network-based) • access extra location provider commands
<u>Normal Permissions</u>	• receive data from Internet • access Bluetooth settings • full network access • prevent device from sleeping • view network connections • pair with Bluetooth devices • run at startup

Overview of Permissions Used

Dangerous permissions used in Mor Chana

Device & app history	- Retrieve running apps
Phone	- Read phone status and identity
Device ID & call information	- Read phone status and identity
Motion and fitness activity	- Control vibration

Use of Permissions

Photos/Media/Files/Storage/Camera

We can see that Mor Chana seeks permission to:

- read the contents of a user's USB storage in their mobile phone
- modify or delete the contents of the USB storage in a user's mobile phone

Justification:

For user to take or upload a selfie during registration.

The privacy statement states that this will not be sent from the phone.

However, we feel that this is *not necessary* – given that the purpose is for contact tracing.

It is unclear how user will share that data with the government if there is in infected case (i.e. no upload button)

Use of Permissions

Phone device information and app history
Device ID and Call Information
Phone

- Retrieve running apps
- Read phone status and identity

Justification
No clear purposes stated in Privacy Statement.
This is excessive to the purpose

Use of Permissions

Location/Contact data via GPS and Bluetooth

- Approximate location (network-based), Precise location (GPS and network-based), access extra location provider commands
- Pair with Bluetooth devices, access Bluetooth settings

Justification

To determine whether user has been in close proximity with an infected individual or area

Not explained explicitly in Privacy Statement, but prompted in-app to ask for user consent

	Thailand
PRIVACY COMMUNICATIONS	Mor Chana
Apps with concerns regarding pre-installation privacy communications	**No Issues** Privacy policy and permissions are easily accessible via GooglePlay/App store/In-App
Apps with excessive permissions based on sweeper's understanding of app's functionality	**Yes**, there are excessive permissions requested within Mor Chana (e.g. Camera, Phone, Device ID)
Apps with privacy communications not well tailored to small screen	**No Issues** Font size is reasonable and layout is clean

OVERALL PRIVACY MARKS	Mor Chana
0 = No privacy information, other than permissions	
1 = Privacy information not adequate; sweeper does not know how information will be collected, used and disclosed	
2 = Privacy information somewhat explains the app’s collection, use and disclosure of personal information; however, sweeper still had questions about certain permissions	Yes
3 = Privacy information clearly explains how app collects/uses/discloses personal information; sweeper is confident in his/her knowledge of app’s practices	

Conclusion

The team behind the Mor Chana app has demonstrated an intention to integrate data protection considerations in its design. However, some permissions do not seem justified.

In addition, the data user intends to further process this data set using analytics. Hence, we recommend a DPIA be conducted and the independent committee be consulted before execution.

StaySafe.ph Review

Edwin Concepcion (FIP, CIPP/E, CIPM, CIPT, GRCP)

Welcome to StaySafe.PH

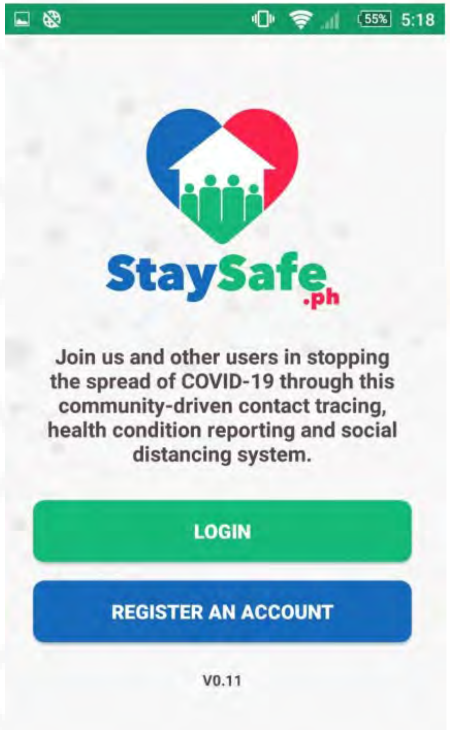
StaySafe.PH is the Philippines official health condition reporting, contact tracing and social distancing system to assist the government on

Stay Healthy. Stay Safe.

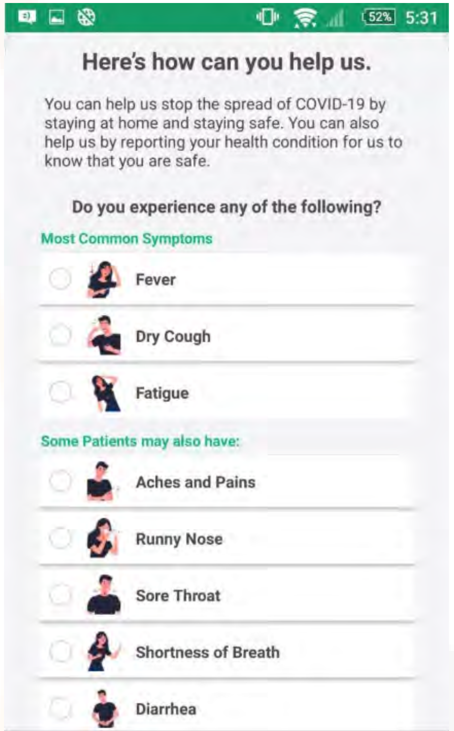
Objectives of StaySafe.ph

The objectives of the StaySafe.ph app are to:

- Community driven contact tracing - allow users to contribute to the national level tracing of COVID-19 by using StaySafe.ph in own communities (by registering or downloading the app).
- Health condition reporting – users reporting their health conditions and also give tips on what to do when one starts experiencing COVID-19 symptoms.
- Social distancing system – maintain social distance by reminding to keep distance from communities with COVID-19 cases by allowing users to scan areas for COVID-19 status



Join us and other users in stopping the spread of COVID-19 through this community-driven contact tracing, health condition reporting and social distancing system.



Here's how can you help us.

You can help us stop the spread of COVID-19 by staying at home and staying safe. You can also help us by reporting your health condition for us to know that you are safe.

Do you experience any of the following?

Most Common Symptoms

○ Fever

○ Dry Cough

○ Fatigue

Some Patients may also have:

○ Aches and Pains

○ Runny Nose

○ Sore Throat

○ Shortness of Breath

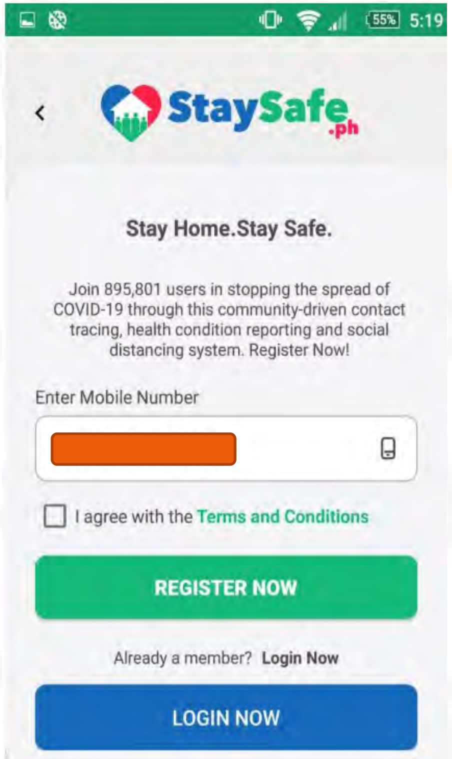
○ Diarrhea

Privacy Notice:

Interagency Task Force (IATF-EID) on Management of Emerging Infectious Diseases and National Task Force (NTF) on COVID-19. The NTF is the Data Controller. Multisys Technologies Corporation as the developer of the website is the Data Processor.

How StaySafe.PH works

- User downloads the app and register his or her mobile phone number. Registration will be confirmed via an OTP.
- The user can provide name, age, location, gender, photo, company name.
- The user is assigned a QR code generated by the app
- User's can turn on mobile phone Bluetooth signals (option).
- User's 'can turn on location (option).
- App retains the information - "for as long as necessary unless you request the deletion of your information, after which these will be securely deleted. However, we may retain your information when required by law".



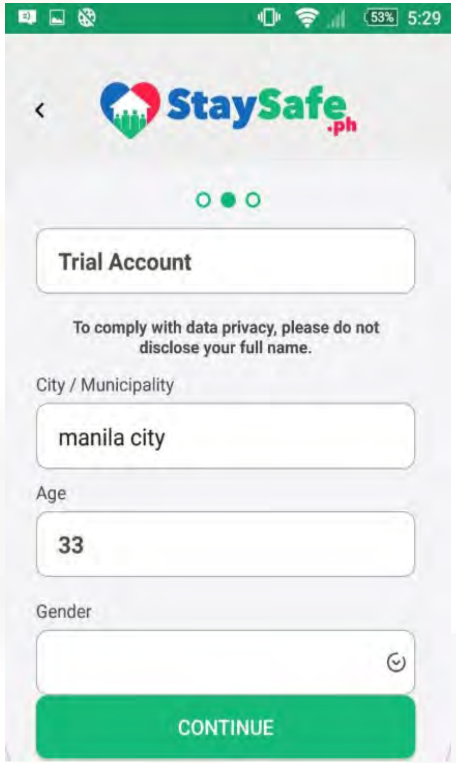
Stay Home.Stay Safe.

Join 895,801 users in stopping the spread of COVID-19 through this community-driven contact tracing, health condition reporting and social distancing system. Register Now!

Enter Mobile Number

[redacted]

□ I agree with the Terms and Conditions



Trial Account

To comply with data privacy, please do not disclose your full name.

City / Municipality

manila city

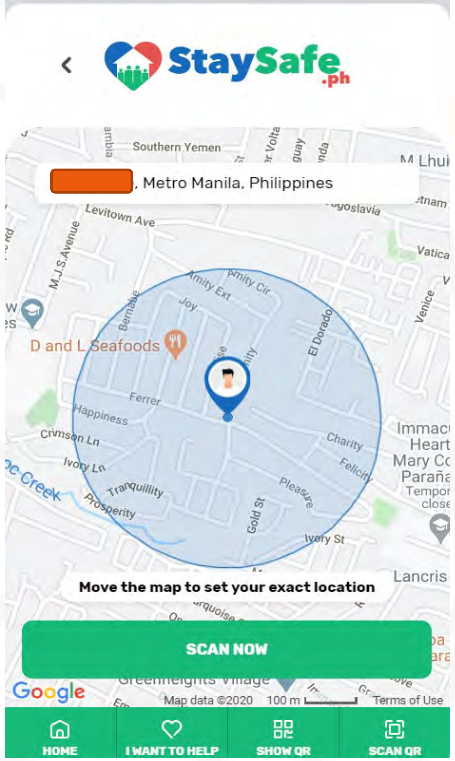
Age

33

Gender

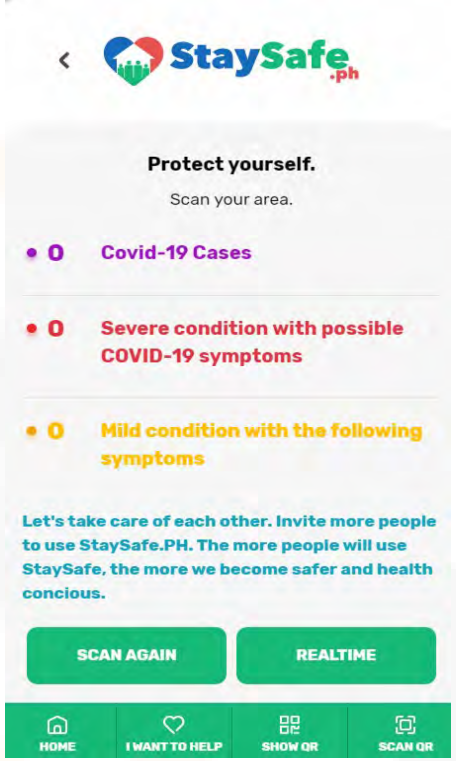
How StaySafe.PH works

- The next stage happens only if:
    - o a user reports his or hear health condition (can include family members)
    - o a user scans the area for COVID-19 status of other users
    - o the app provides COVID-19 "status update" of scanned area
- StaySafe.ph collects reported health condition and provide user with basic medical information and the recommended actions of the DOH based on your condition.
- StaySafe.ph uses geolocation, when enabled by the user, to facilitate contact tracing. The system uses the built-in Bluetooth signals in the mobile phones of users, which allows them to exchange IDs with anonymity, encrypted on the devices.
- StaySafe.ph uses the information to compile reports added to the "heatmap" dashboard of the admin.
- The national government is given "Super Admin" access with a dashboard that can track COVID-19 cases on a national level.



[redacted], Metro Manila, Philippines

Move the map to set your exact location



Protect yourself.

Scan your area.

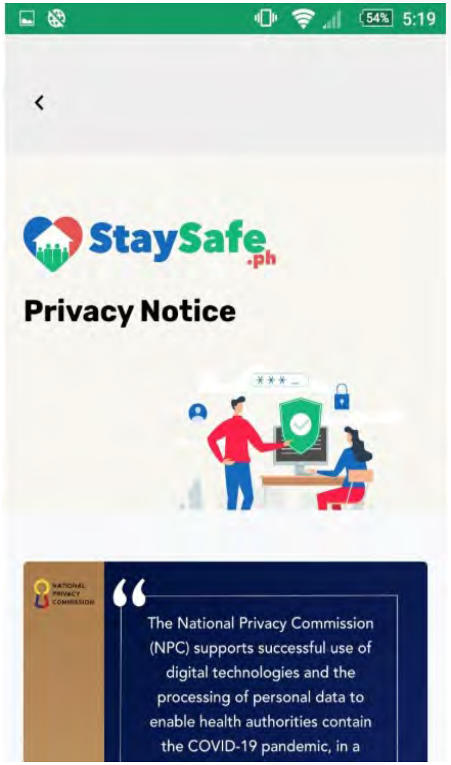
● 0 Covid-19 Cases

● 0 Severe condition with possible COVID-19 symptoms

● 0 Mild condition with the following symptoms

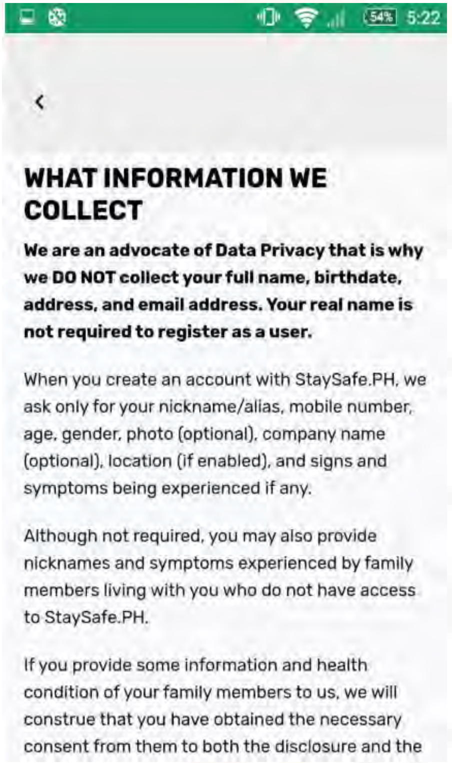
Let's take care of each other. Invite more people to use StaySafe.PH. The more people will use StaySafe, the more we become safer and health concious.

StaySafe.PH Privacy Notice



Privacy Notice

“The National Privacy Commission (NPC) supports successful use of digital technologies and the processing of personal data to enable health authorities contain the COVID-19 pandemic, in a



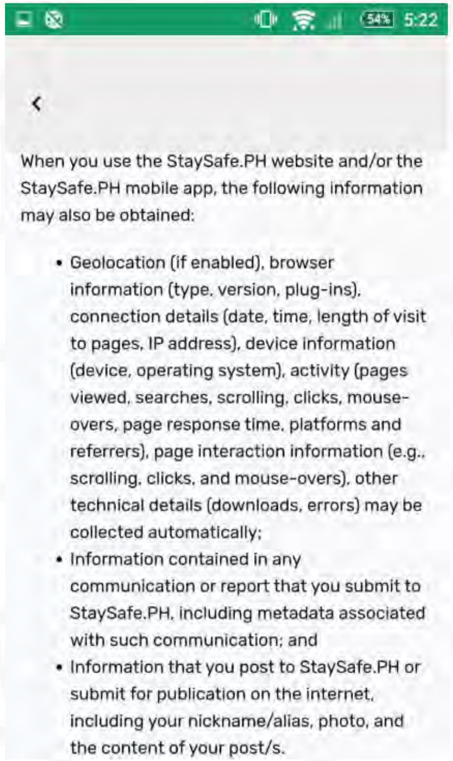
WHAT INFORMATION WE COLLECT

We are an advocate of Data Privacy that is why we DO NOT collect your full name, birthdate, address, and email address. Your real name is not required to register as a user.

When you create an account with StaySafe.PH, we ask only for your nickname/alias, mobile number, age, gender, photo (optional), company name (optional), location (if enabled), and signs and symptoms being experienced if any.

Although not required, you may also provide nicknames and symptoms experienced by family members living with you who do not have access to StaySafe.PH.

If you provide some information and health condition of your family members to us, we will construe that you have obtained the necessary consent from them to both the disclosure and the



When you use the StaySafe.PH website and/or the StaySafe.PH mobile app, the following information may also be obtained:

- Geolocation (if enabled), browser information (type, version, plug-ins), connection details (date, time, length of visit to pages, IP address), device information (device, operating system), activity (pages viewed, searches, scrolling, clicks, mouse-overs, page response time, platforms and referrers), page interaction information (e.g., scrolling, clicks, and mouse-overs), other technical details (downloads, errors) may be collected automatically;
- Information contained in any communication or report that you submit to StaySafe.PH, including metadata associated with such communication; and
- Information that you post to StaySafe.PH or submit for publication on the internet, including your nickname/alias, photo, and the content of your post/s.

- Privacy information somewhat explains the app’s collection, use and disclosure of personal information; however, sweeper still had questions about certain permissions
- Personal data is retained “for as long as necessary”.
- StaySafe.ph “Privacy notice” is somewhat confusing.
- Multisys Technologies Corporation (develop and data processor) provided a narrative in their own website - All-in-one: Eight elaborate features of contact tracing platform StaySafe.ph https://www.multisyscorp.com/news/all-in-one-eight-elaborate-features-of-contact-tracing-platform-staysafeph
- Multisys Technologies Corporation has no “privacy notice” on its website

Overview of Permissions Used

Dangerous permissions used in StaySafe.PH

Photos/Media/ Files	• read the contents of your USB storage • modify or delete the contents of your USB storage
Storage	• read the contents of your USB storage • modify or delete the contents of your USB storage
Location	• approximate location (network-based) • precise location (GPS and network-based)
Camera	• Takes pictures and videos • Scan QR code
Normal	• receive data from Internet • access Bluetooth settings • full network access • Via network connections • prevent device from sleeping • view network connections • pair with Bluetooth devices • run at start-up • control vibration • may update to StaySafe.PH

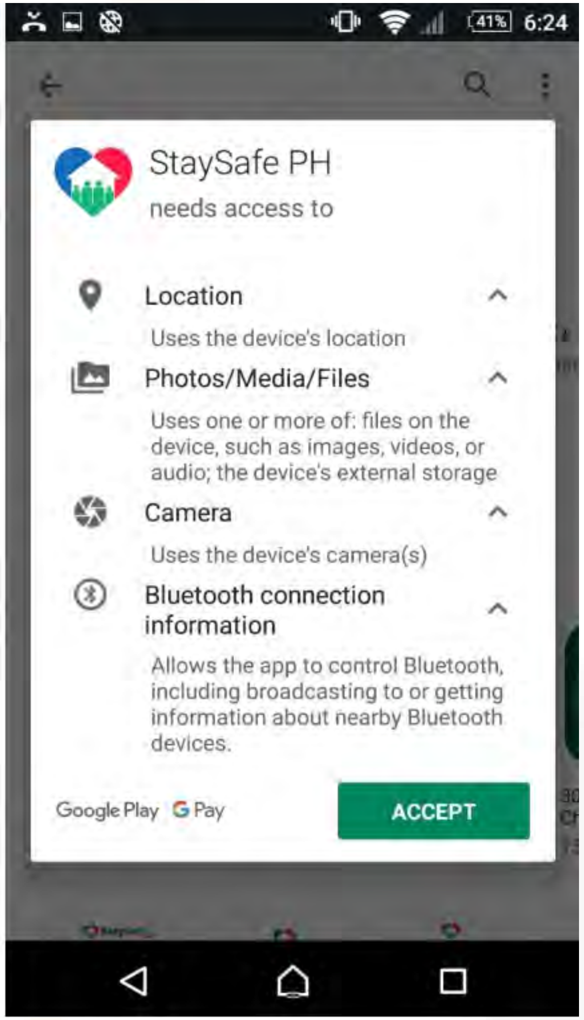
Use of Permissions

Photos/Media/Files/Storage

- We can see that StaySafe.PH seeks permission to:
  - modify or delete the contents of the USB storage in a user’s mobile phone
  - read the contents of a user’s USB storage in their mobile phone

<u>Justification</u>:

- Permissions are sought so that the app can store ‘close proximity’ information. This means that the ‘close proximity’ information can be read if it becomes necessary to trace the user’s contacts.
- The health reports submitted is also added to the “heatmap” dashboard of the admin—an analytics feature that shows the areas with worsening or improving rate of COVID-19 cases.



StaySafe PH
needs access to

Location
Uses the device's location

Photos/Media/Files
Uses one or more of: files on the device, such as images, videos, or audio; the device's external storage

Camera
Uses the device's camera(s)

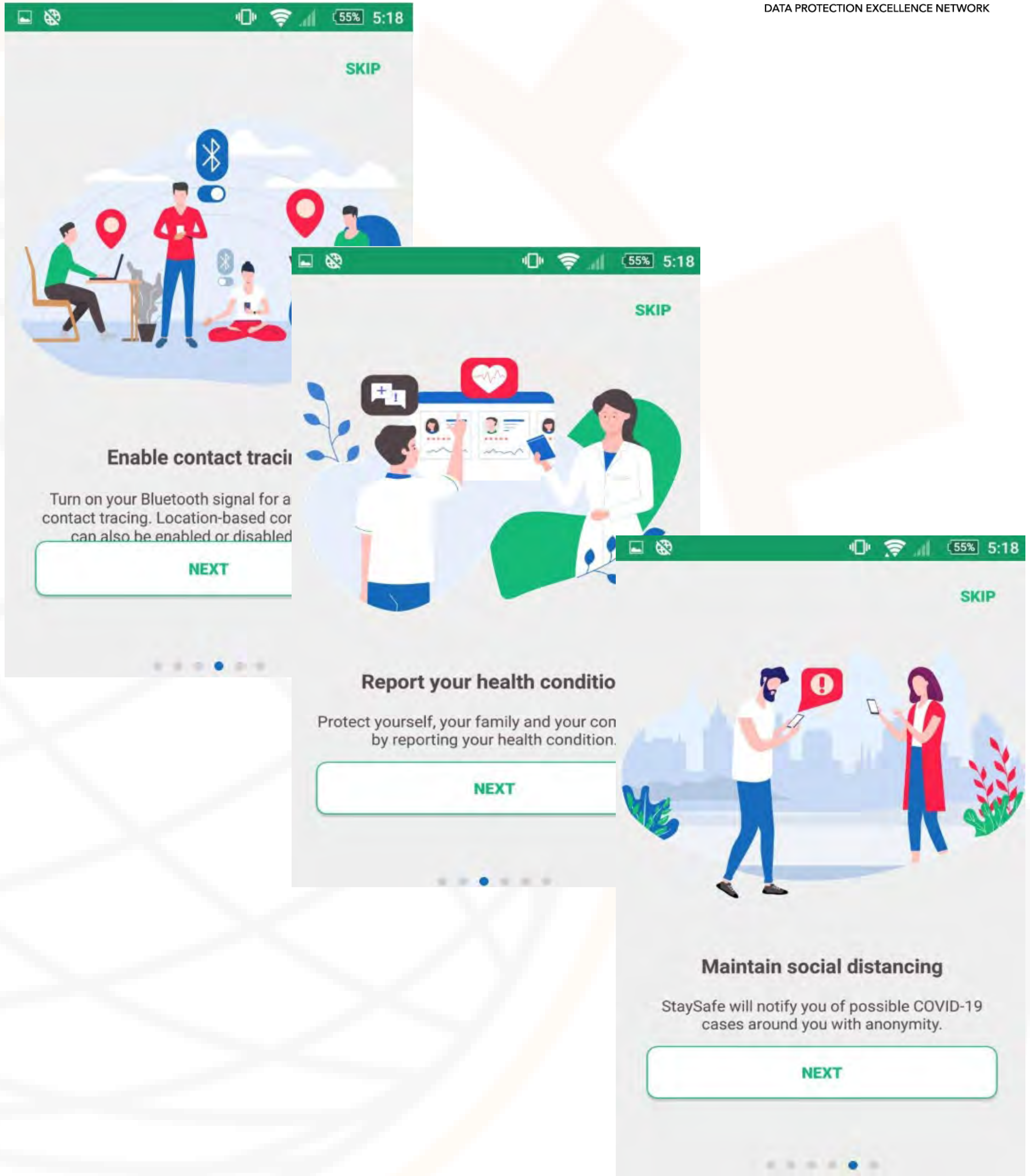
Bluetooth connection information
Allows the app to control Bluetooth, including broadcasting to or getting information about nearby Bluetooth devices.

Use of Permissions

Photos/Media/Files/Storage

The privacy statement in the StaySafe.PH app says that:

- We collect your information to enable you to report your (including family members you register) health condition and provide you with basic medical information and the recommended actions of the DOH based on your condition.
- Multisys Technologies Corporation provides more details on StaySafe.ph mobile application on the contact tracing, scan area features - “The mobile app has a contact tracing feature that determines when a user’s phone is near another that has also installed the app. The system uses the built-in Bluetooth signals in the mobile phones of users, which allows them to exchange IDs with anonymity, encrypted on the devices”. https://www.multisyscorp.com/news/staysafeph-mobile-application-with-contact-tracing-scan-area-features-now-on-google-play



Enable contact traci

Turn on your Bluetooth signal for a
contact tracing. Location-based cor
can also be enabled or disabled

Report your health conditio

Protect yourself, your family and your con
by reporting your health condition.

Maintain social distancing

StaySafe will notify you of possible COVID-19 cases around you with anonymity.

Use of Permissions

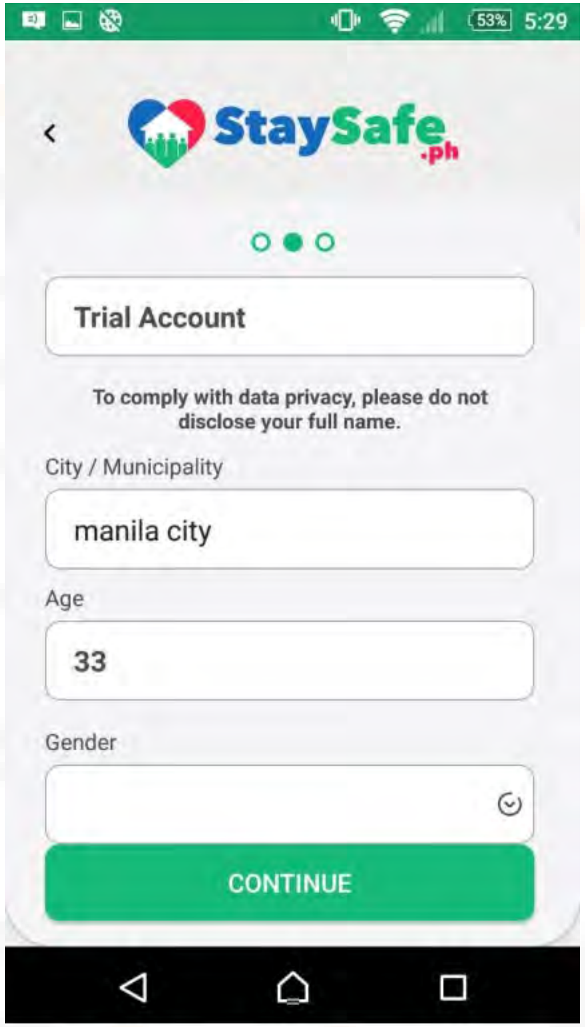
Location

According to the privacy statement for the StaySafe.ph app:

- Your location, when enabled by you, is collected to facilitate the Government in contact tracing.
- StaySafe.ph privacy statement does not say anything specific how it use device Bluetooth feature
- Provides separate explanation on Multisys Technologies Corporation website.

The statement about location is inconsistent with the permissions listed (for which consent is sought by the app when downloading it):

- approximate location (network-based)
- precise location (GPS and network-based)



Trial Account

To comply with data privacy, please do not disclose your full name.

City / Municipality

manila city

Age

33

Gender

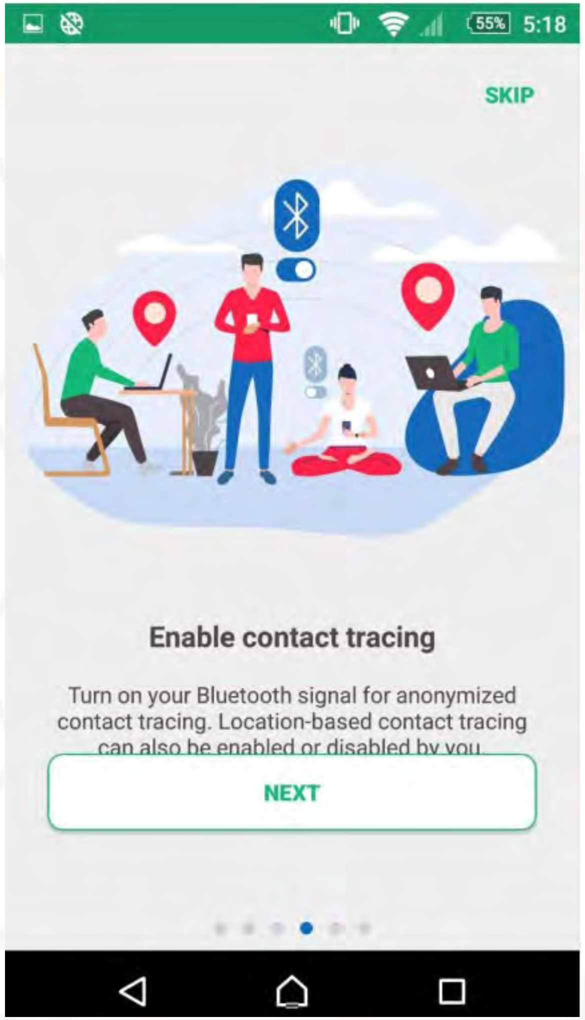
Use of Permissions

Location

- This inconsistency arises because:
    - Location permissions are mandatory when Bluetooth technology is used.
    - It is an outcome of how the Bluetooth technology works - the location permission is required so that 'close proximity' information can be collected.

- No confirmation that the app does NOT collect and store the location data used in relation to the 'close proximity' information.

- The privacy statement does not make this clarification, which could be confusing to a non-technical user.



Enable contact tracing

Turn on your Bluetooth signal for anonymized contact tracing. Location-based contact tracing can also be enabled or disabled by you.

Use of Permissions

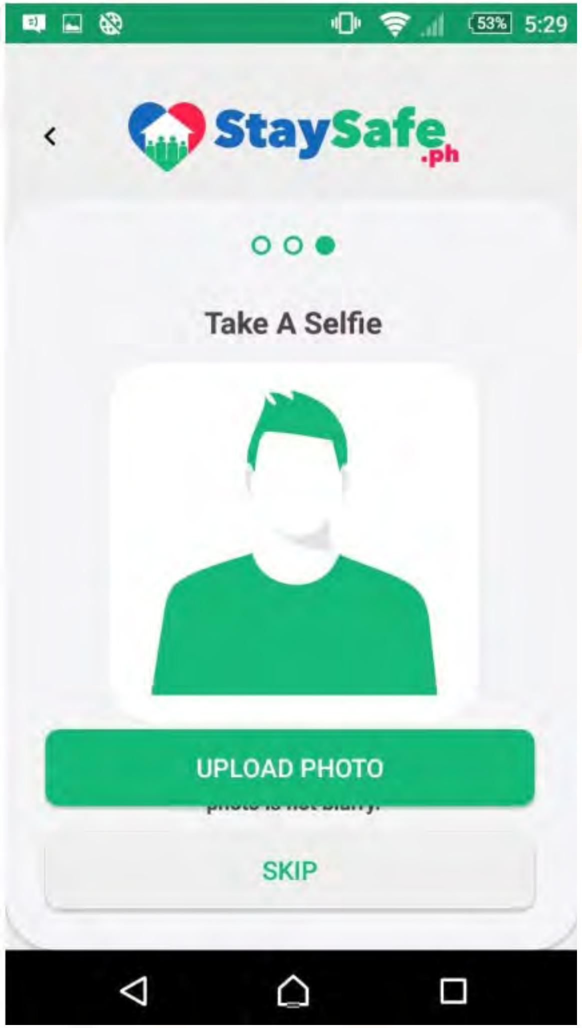
Camera

According to the privacy statement for the StaySafe.ph app:

- When you use the StaySafe.PH website and/or the StaySafe.PH mobile app, the following information may also be obtained:
  - Geolocation (if enabled), browser information (type, version, plug-ins), connection details (date, time, length of visit to pages, IP address), device information (device, operating system), activity (pages viewed, searches, scrolling, clicks, mouse-overs, page response time, platforms and referrers), page interaction information (e.g., scrolling, clicks, and mouse-overs), other technical details (downloads, errors) may be collected automatically;
- In Multisys website: "StaySafe.ph generates unique QR codes for users that can be utilized by local government units (LGUs) as an alternative to the traditional printed quarantine passes, which users may present for future health checks and contact tracing."

The statement about camera is lacking with the permissions listed (for which consent is sought by the app when downloading it):

- To generate and use of the QR code
- To upload photo

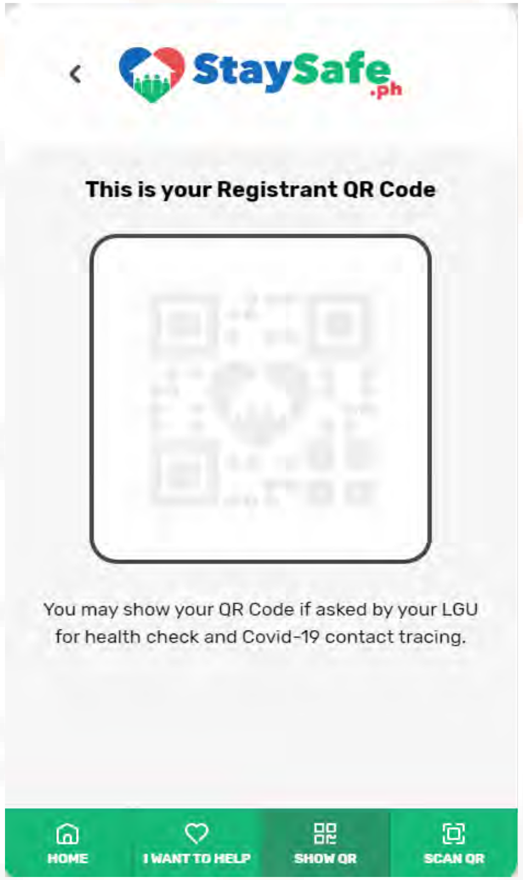


Use of Permissions

Camera

- The lack of explanation does not provide clarity to the:
    - Necessity in generating the QR code
    - It is an outcome of how the QR code can be utilized as quarantine pass

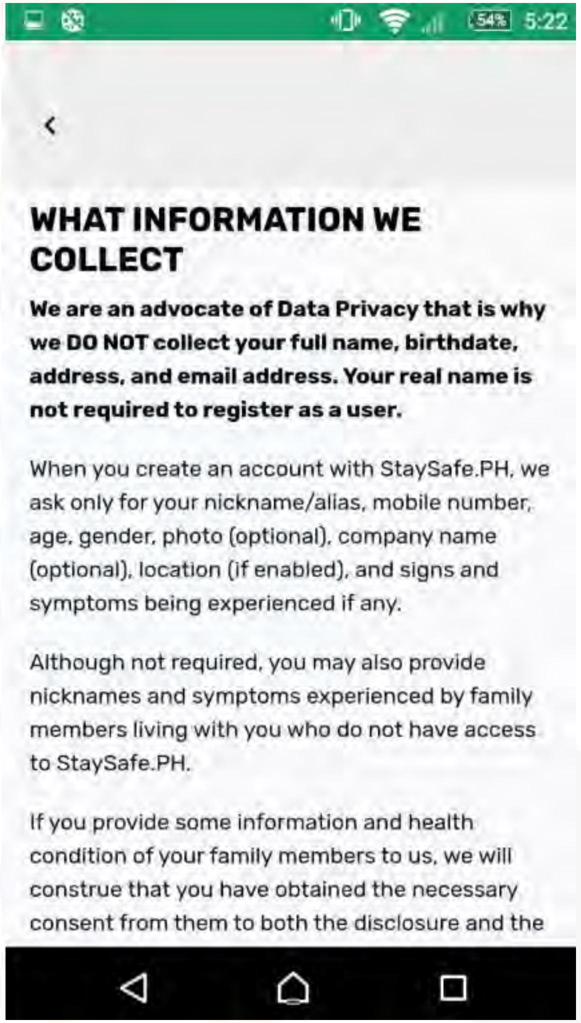
- The privacy statement does not make this clarification, which could be confusing to a non-technical user.



This is your Registrant QR Code

You may show your QR Code if asked by your LGU for health check and Covid-19 contact tracing.

	Philippines
PRIVACY COMMUNICATIONS	StaySafe.PH
Apps with concerns regarding pre-installation privacy communications	**Inconsistent** (Multisys: All-in-One)
Apps with excessive permissions based on sweeper's understanding of app's functionality	**No issues**
Apps with privacy communications not well tailored to small screen	**No Issues**



WHAT INFORMATION WE COLLECT

We are an advocate of Data Privacy that is why we DO NOT collect your full name, birthdate, address, and email address. Your real name is not required to register as a user.

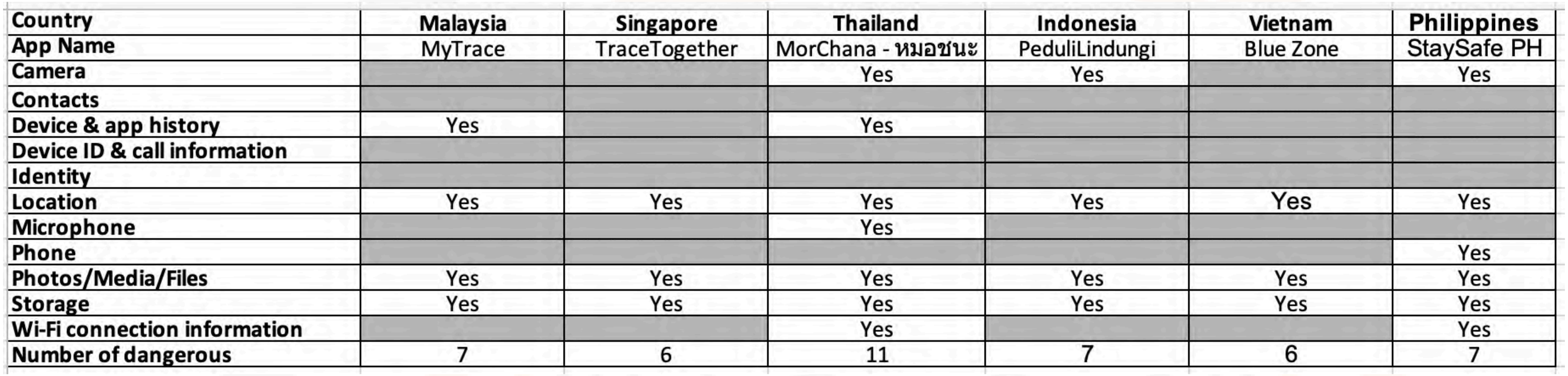
When you create an account with StaySafe.PH, we ask only for your nickname/alias, mobile number, age, gender, photo (optional), company name (optional), location (if enabled), and signs and symptoms being experienced if any.

Although not required, you may also provide nicknames and symptoms experienced by family members living with you who do not have access to StaySafe.PH.

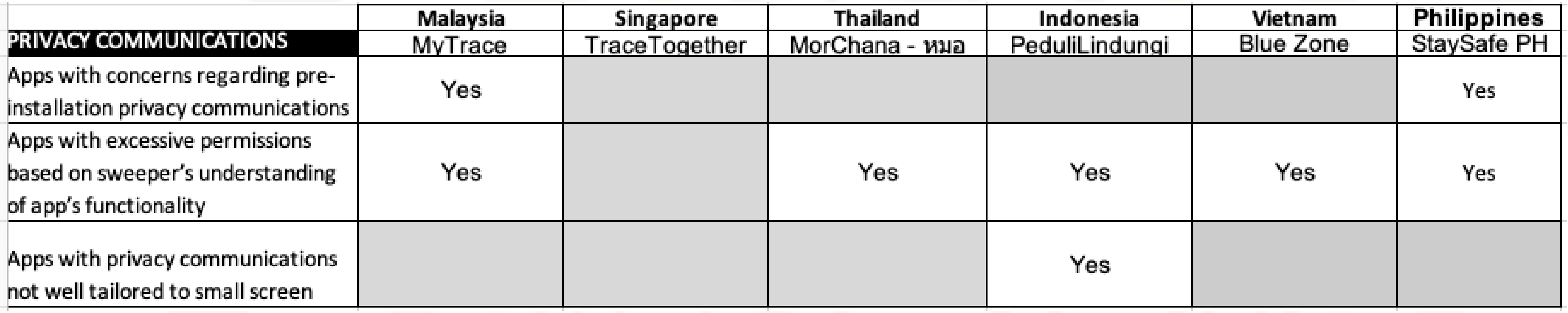
If you provide some information and health condition of your family members to us, we will construe that you have obtained the necessary consent from them to both the disclosure and the

OVERALL PRIVACY MARKS	StaySafe.ph
0 = No privacy information, other than permissions	
1 = Privacy information not adequate; sweeper does not know how information will be collected, used and disclosed	
2 = Privacy information somewhat explains the app’s collection, use and disclosure of personal information; however, sweeper still had questions about certain permissions	Yes
3 = Privacy information clearly explains how app collects/uses/discloses personal information; sweeper is confident in his/her knowledge of app’s practices	

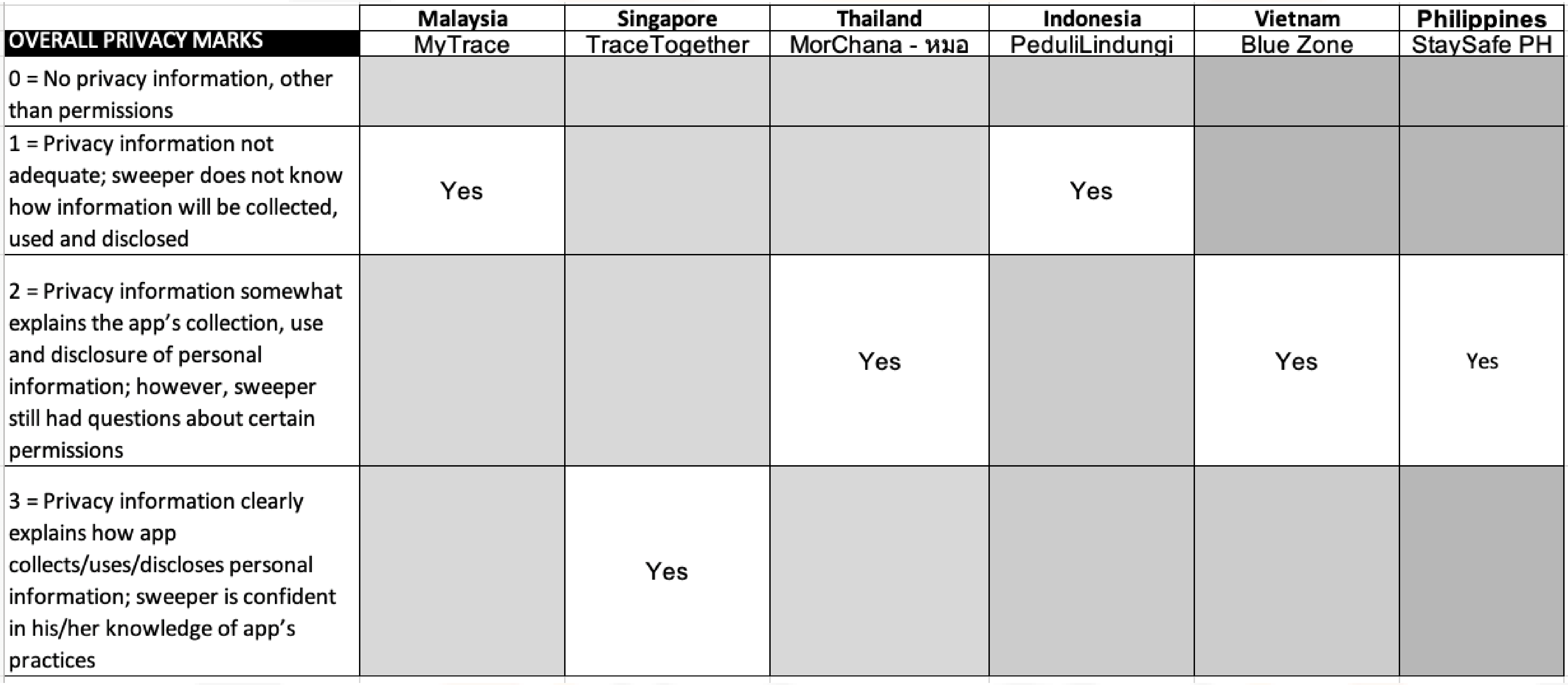
Comparison Among Contract Tracing Apps in ASEAN



Country	Malaysia	Singapore	Thailand	Indonesia	Vietnam	Philippines
App Name	MyTrace	TraceTogether	MorChana - หมอชนะ	PeduliLindungi	Blue Zone	StaySafe PH
Camera			Yes	Yes		Yes
Contacts						
Device & app history	Yes		Yes			
Device ID & call information						
Identity						
Location	Yes	Yes	Yes	Yes	Yes	Yes
Microphone			Yes			
Phone						Yes
Photos/Media/Files	Yes	Yes	Yes	Yes	Yes	Yes
Storage	Yes	Yes	Yes	Yes	Yes	Yes
Wi-Fi connection information			Yes			Yes
Number of dangerous	7	6	11	7	6	7



	Malaysia	Singapore	Thailand	Indonesia	Vietnam	Philippines
PRIVACY COMMUNICATIONS	MyTrace	TraceTogether	MorChana - หมอ	PeduliLindungi	Blue Zone	StaySafe PH
Apps with concerns regarding pre-installation privacy communications	Yes					Yes
Apps with excessive permissions based on sweeper's understanding of app's functionality	Yes		Yes	Yes	Yes	Yes
Apps with privacy communications not well tailored to small screen				Yes		



	Malaysia	Singapore	Thailand	Indonesia	Vietnam	Philippines
OVERALL PRIVACY MARKS	MyTrace	TraceTogether	MorChana - หมอ	PeduliLindungi	Blue Zone	StaySafe PH
0 = No privacy information, other than permissions						
1 = Privacy information not adequate; sweeper does not know how information will be collected, used and disclosed	Yes			Yes		
2 = Privacy information somewhat explains the app's collection, use and disclosure of personal information; however, sweeper still had questions about certain permissions			Yes		Yes	Yes
3 = Privacy information clearly explains how app collects/uses/discloses personal information; sweeper is confident in his/her knowledge of app's practices		Yes				

Conclusion

- Key to understanding privacy is to examine the “dangerous” permissions at the app level and compare them against the specific purposes and functionalities of the App. These need to be consistent to what is stated in the privacy notice, terms and conditions as well as the help documentation.
- Singapore’s TraceTogether contact tracing app came up as least intrusive in terms of privacy communication permissions and topped overall privacy marks.
- Countries like Indonesia and Vietnam have not yet passed data protection laws. Hence, we see less focus on addressing privacy concerns.
- Better oversight is recommended when a third party app developer is being used by the government (which may be a case in The Philippines). A Data Protection Impact Assessment (DPIA) is crucial to identify privacy and security risks

THANK YOU!