

COVID-19 Webinar

COVID-19 and the Impact on Data Privacy

Data Protection Excellence Network

14 April 2020



INTRODUCTION

Kevin Shepherdson, CEO, Straits Interactive

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

Agenda

- Introduction
- COVID-19 updates in the ASEAN region
- Q&A on Country Updates
- TraceTogether Review
- Close

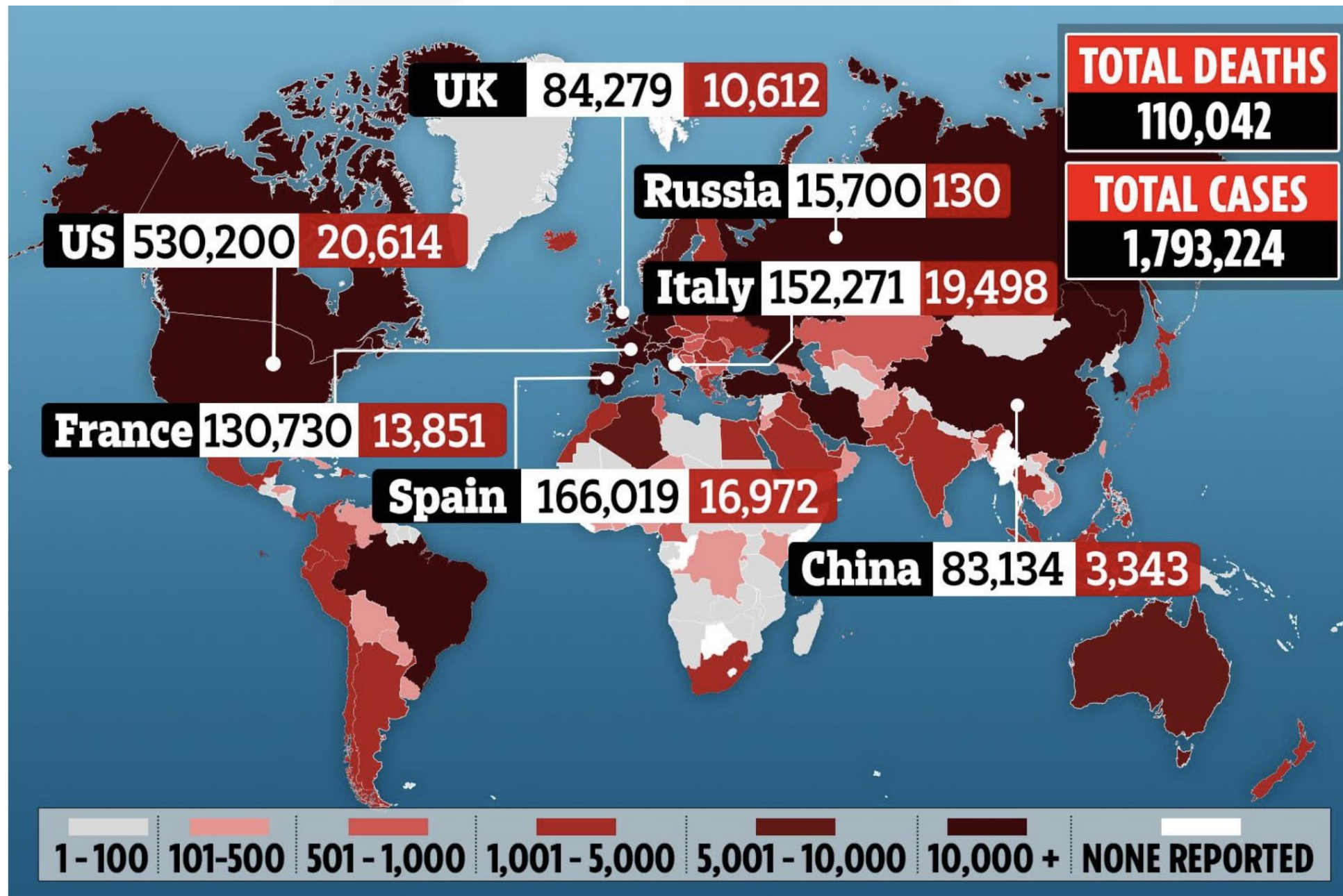
Speakers

- **Lyn Boxall** (FIP, CIPP/E, CIPP/A, CIPM, GRCP, GRCA), Lyn Boxall LLC
- **William Hioe** (FIP, CIPP/E, CIPP/A, CIPM, CIPT, GRCP), Head, Regional Consultancy, Straits Interactive
- **Jon Bello** (FIP, CIPP/E, CIPM), Chair, KnowledgeNet, IAPP
- **Dr Prapanpong Khumon** Associate Dean at School of Law, University of the Thai Chamber of Commerce,
- **Dr Sonny Zulhuda**, Civil Law Department, Ahmad Ibrahim Kulliyah of Laws, the International Islamic University Malaysia

WUHAN CHINA – THE GENESIS

- **DEC. 31,2019** the government in Wuhan, China, confirmed that health authorities were treating dozens of cases.
- **JAN. 23** - Wuhan, a city of more than 11 million, was cut off by the Chinese authorities.
- **JAN 30th** - The W.H.O. declared a global health emergency.
- **FEB. 7:** A Chinese doctor who tried to raise the alarm died.
- **FEB. 11** - The disease the virus causes got a new name (COVID19)
- **APR 8** : Wuhan, the epicentre of the outbreak finally lifted the 76-days lockdown - Life in China is gradually going back to normal
- **Till date** : Total infections number 83597 cases, 78145 has recovered, with only 2101 active cases now.

Study suggests that over 1.4 million infections and 56,000 deaths might have been avoided as a result of these effective control measures



CONFIRMED COVID-19 CASES AND DEATHS IN ASEAN



		Total Cases	New Cases	Total Deaths	New Deaths	Total Recovered
Philippines		4,932	+284	315	+18	242
Malaysia		4,817	+134	77	+1	2,276
Indonesia		4,557	+316	399	+26	380
Thailand		2,579	+28	40	+2	1,288
Singapore		2,532	+233	8	0	560
Vietnam		262	+4	0	0	145
Brunei		136	0	1	0	107
Cambodia		122	0	0	0	77
Myanmar		41	+3	4	+1	2
Lao PDR		19	0	0	0	0
ASEAN		19,997	+1,002	844	+48	5,077

*Source: WHO et. al. as at 7:00PM GMT +8 dated 13 April 2020.

Summary : Government Measures

Governments have implemented the following preventative and safety measures:

- **Conducting surveillance activities**, including contact tracing whenever an infection is reported
- **Quarantining individuals**, including in isolation wards in hospitals when they have been diagnosed as having been infected with COVID-19 and in home isolation when they have been in close contact with an infected individual
- **Monitoring that individuals required to be in home isolation** comply with the relevant requirements , among other business and community guidelines

Summary : Organisational Measures

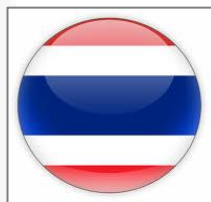
Typical activities that organisations have implemented as preventative and safety measures regarding COVID-19 (before lockdown):

- **Requiring staff and visitors to submit to temperature checks and to declare any medical symptoms of 'flu before entering the organisation's premises**
- **Requiring staff and visitors to answer questions about whether or not they have been to countries with a large number of COVID-19 infection cases, or in contact with other infected individuals**
- **Implementing flexi-office or remote working arrangements with the intention of minimising the risk to themselves of exposure to infection (for example, during their commute to the office) and minimising the risk to others (such as their office colleagues) of exposure to infection**
- **Responding to medical emergencies (for example, where a staff falls ill and medical assistance needs to be called in)**

What is the Impact on Data Privacy in the ASEAN region?

ASEAN COUNTRY UPDATES

- Current Status of COVID (lockdown or partial)
- Overall precautions being taken / got initiatives
- What the laws permits / requires
- What role the data protection regulator is taking
- Incidents (good and bad privacy practices)
- How the balancing between privacy and public safety is turning out



Covid-19 and the Impact to Data Privacy

Thailand's Perspective

Prapanpong Khumon

Associate Dean

School of Law, University of the Thai Chamber of Commerce



Agenda

- Situations and overall precautions
- Legal grounds
- Incidents in relation to data privacy practices
- Balancing interests between privacy and public safety

1. Situations and overall precautions

Thailand – Partial lockdown

Disclosing information on reported COVID-19 cases

- For public information: identifiable personal information is not disclosed, the set of information disclosed is, for example, gender, age, recent places where such person has been to.
- For workplace communications: internal communications and updates (but do not give out names and job titles).
- For medical treatment: transfer patient’s information to another hospital for treatment or diagnostic purpose.
- For duty to notify suspicious cases: home owners, hospital staff, or employer shall report suspicious case to a relevant authority (a disease control officer).

Tracking inbound travellers entering Thailand

- Both Thai and foreign travellers entering to Thailand to download “AOT Airport” Application on their mobile phones.
- This application will track them for two main purposes:
 - For Thai health officials to contact them in case of an emergency, e.g., informing if passengers seated in close vicinity are tested positive for COVID-19
 - For monitoring 14 days self-quarantine (e.g. will alert officials if a person leaves the designated quarantine area)
- The personal data will be deleted 14 days after arrival.



2. Legal grounds

Personal Data Protection Act of Thailand (PDPA 2019 – to be effective 27 May 2020)

Processing of personal data without obtaining consent from an individual is allowed in an event of epidemic prevention when:

- Necessary to carry out task for public interest - art 24(4)
- Protecting public health and prevention of an epidemics - art 25(5)
- In both cases, for sensitive personal data:
 - It must be necessary for compliance with law that specifies such purpose and
 - Must ensure there are suitable safeguards to the right and freedom of the data subject

Laws on public health/ emergency in epidemic prevention

Tracking and monitoring - tracking applications may be utilized via mobile phones for disease prevention (Section 11 of Regulation issued under Article 9 of the Emergency Decree on Public Administration in Emergency Situations issued on 26 March 2020)

Disclosing personal information - duty to notify suspicious cases to a relevant authority (Notification of the Ministry of Public Health No. 134 on 21 December 2017) and officials must keep confidential and can only be disclosed in a limited circumstances (Section 10 of the Communicable Disease Act 2015)

Transfer patient's information to another place/ hospital - for treatment or diagnostical purpose in accordance with guidance issued by the Ministry of Public Health (Notification on Ministry of Public Health No. 137 on 4 March 2020)

3. Incidents in relation to data privacy practices

- In early April, personal data of more than 100 persons who disobeyed the quarantine order have been revealed to public (incl. names, address) but such personal data has been taken out of platforms a few days after the release.
- This voluntary self-censorship may come from a community pressure or comments of privacy watchdog (NGO) as Thailand is yet to set up the data protection regulator (scheduled within this year) because the PDPA is not in force yet.

4. Balancing interests between privacy and public safety

- When the Thai PDPA is not in force yet, professional/community guidelines can play a part in ensuring authorities do not go too far on privacy intrusion.
- Ensure that professional/ committee guidelines are being implemented when handling personal data in times of epidemics.
- Ensure that the use is not excessive and there is the security of personal data in place when using tracking applications, and personal data should be destroyed when the purpose is fulfilled.

THANK YOU!



Prapanpong Khumon



prapanpong_khu@utcc.ac.th



School of Law, University of the Thai Chamber of
Commerce, Thailand



DPEX

DATA PROTECTION EXCELLENCE NETWORK



Covid-19 and the Impact to Data Privacy

The Philippines' Situation

Jon Bello CIPM/CIPPE/FIP



The Philippine Situation

Current Status of Lockdown

- Enhanced Community Quarantine (March 16 to April 30, Luzon) – Closure of Establishments, Social Distancing, and Curfew Hours
- Exception : Essential Services and other Exempted Entities (Hospitals, Telcos, Supermarkets, Banks, BPOs, etc.)
 - Skeletal Workforce
 - Work at Home Arrangements

The Philippine Situation

Overall Precautions Being Taken/Initiatives

- Contact Tracing by the Department of Health (Close contact with an infected person)
- Reporting of Persons Suspected as having Covid-19 in establishments such as Workplaces, Schools, Residential Communities, Hotels (Temperature Checks, Survey Forms/Travel History)

The Philippine Situation

Data Privacy Act of 2012 and IRR

Sensitive Personal Info- Health Data (Contact List/Case Investigation Form)

Basis for Processing:

1. Consent
2. Vital Interest

3. Public Authority (Exemption)/Legal Obligation

- RA 11332 (*Mandatory Reporting of Notifiable Diseases and Health Events of Public Concern Act*)
- RA 11058 (*Act Strengthening Compliance with Occupational Safety and Health Standards and Providing Penalties for Violations*); Labor Advisory No. 4, Series of 2020

The Philippine Situation

Role of Data Protection Regulator

The *National Privacy Commission* as an advocate of the balance of privacy rights and public interest:

NPC PHE Bulletin No. 1 – Release of Passenger Manifest to Govt

NPC PHE Bulletin No. 2 – Upholding Patient Confidentiality and Privacy Rights during a Public Health Emergency

NPC PHE Bulletin No. 3: Collect what is necessary; Disclose only to the proper authority (FAQs)

NPC PHE Bulletin No. 5: “Social Vigilantism”

NPC PHE Bulletin No. 7: On Calls for Patients to Waive Privacy Rights, Publicly Disclose Health Status

The Philippine Situation

Privacy Issues

Case No. 1 Unauthorized Disclosure by a Hospital Employee on Social Media/Homeowners' Association

Case No. 2 Discrimination against persons with Covid19 (Publicly Identified by the LGU w/ consent)

Case No. 3 Contract Tracing Sites/Apps that collect excessive personal data

Best Practices

1. Remember the Principles: Transparency, Legitimate Purpose, Proportionality.
2. Employee Training and Awareness on Policies (including those on WAH arrangements)
3. Contract Tracing Sites/Apps will need to be scrutinized (security measures/retention)
4. Be ready for a Data Subject's exercise of rights

The Philippine Situation

The Balance Between Privacy and Public Safety

1. Draft Resolution No. 22 of the Inter-Agency Task Force:

“The IATF adopts the policy of mandatory public disclosure of personal information relating to positive COVID-19 cases to enhance the contact tracing efforts of the government.”


2. Joint Statement of the Integrated Bar of the Philippines, Philippine Medical Association, and Philippine College of Surgeons: “Public Health Safety Prevails Over Confidentiality of Medical Data.”


3. Openness to Surveillance for Contact Tracing Purposes (3 providers in the P Philippines; Apple and Google Team Up)

4. The Employers’ Obligation to Provide Healthy and Safe Working Environment

THANK YOU!

 Jon Bello CIPM/CIPPE

 jbello1217@gmail.com

 63 9209212712



Covid-19 and the Impact to Data Privacy Singapore

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

William Hioe (FIP, CIPP/E, CIPP/A, CIPM, CIPT, GRCP),
Head, Regional Consultancy, Straits Interactive



Country Updates - Singapore

Current Status of COVID-19 – as at midnight 13 April 2020

New cases: 386

- Imported: 0
- Linked to known clusters: 280 (majority Work Permit Holders in dorms)
- Linked to other cases: 12 (7 S'pore Citizens/PRs, 5 Work Permit holders)
- Pending contact tracing: 94 (21 S'pore citizens/PRs; 73 S Pass/Work Permit/Long Term Pass holders)

Total cases: 2,918

- Hospitalised: 1,158 (29 in ICU)
- In community facilities: 1,165
- Fatalities: 9
- Total discharged: 586 (Discharged today: 26)

Country Updates - Singapore

Current Status of COVID-19 – ‘Circuit Breaker’ Restrictions

Lockdown:

The general rule is that everyone must stay at home and not have any contact outside their own household.

Exceptions include:

- workers in essential services can go to work – all non-essential businesses are shut
- one household member can go out to buy essential items, such as food
- non-routine visits to clinics for treatment
- visits to elderly people who are in need of assistance
- exercise, but social distancing rules must be followed

When not at home, everyone must wear a mask.


Country Updates - Singapore

The government has been very active in providing information:

 Websites on COVID-19 situation: MOH: moh.gov.sg/covid-19; Gov.sg: gov.sg/features/covid-19


 Receive updates on the go: go.gov.sg/whatsapp; go.gov.sg/govsg-telegram


 COVID-19 Info Bot - a repository of answers to your questions on latest measures

 Summarised info from different govt agencies, organised into topics that are of interest to you
gov.sg/infobot

 Sick? Find a PHPC clinic near you: phpc.gov.sg;  COVID-19 online symptom checker
sgcovidcheck.gov.sg

 Installing TraceTogether app: tracetogether.gov.sg

 Check how crowded malls/parks are before going: www.spaceout.gov.sg;
safedistparks.nparks.gov.sg

 Hotlines: MOH COVID-19 hotline 1800 333 9999; National CARE hotline - for those facing anxiety and stress: 6202 6868

Country Updates - Singapore

What the law permits / requires

- Regulations have been made under the Infectious Diseases Act – ‘circuit breaker’ restrictions.
- The COVID-19 (Temporary Measures) Act 2020 was passed on 7 April 2020 and came into effect on 8 April 2020.
- The COVID-19 (Temporary Measures) (Control Order) Regulations 2020 were made by the Minister of Health and took effect on 10 April 2020.
- Employers are under an obligation to provide employees with a safe workplace – this is part of Singapore’s laws on workplace safety and health.
- The Personal Data Protection Act 2012 governs the way in which organisations can collect, use or disclose personal data.

Country Updates - Singapore

Role of the Personal Data Protection Commission of Singapore

On www.pdpc.gov.sg:

NOTICE: The PDPC office is closed until further notice, in view of the stricter safe-distancing measures. Should you urgently require to meet our officers, please write to info@pdpc.gov.sg to make an appointment.

Country Updates - Singapore

Role of the Personal Data Protection Commission of Singapore

On 13 February 2020, the Commission issued an **Advisory on Collection of Personal Data for COVID-19 Contact Tracing**. The Commission said that:

- organisations may collect personal data of visitors to their premises for the purposes of contact tracing and other response measures in the event of an emergency, such as during the COVID-19 outbreak
- relevant personal data can be collected, used and disclosed **without consent** for contact tracing and other response measures, as this is necessary to respond to an emergency that threatens the life, health or safety of other individuals
- as organisations need to accurately identify individuals in these circumstances, they may collect visitors National Registration Identity Card (NRIC) number, foreign identification number (FIN) or passport number for this purpose
- The Commission added a reminder: organisations that collect such personal data must comply with the data protection provisions of the PDPA.

Country Updates - Singapore

Incidents - as reported in The Straits Times on 14 April 2020

Headline: 'Coronavirus: More than 200 fines issued for flouting of elevated safe distancing rules.'

More than 200 fines of \$300 each were issued to those who flouted elevated safe distancing measures on Monday April 13, said the Ministry of the Environment and Water Resources.

Among those fined is a woman who sat on a marked seat at a food centre in Aljunied.



Country Updates - Singapore

Balancing between privacy and public safety

- There is an elevated level of surveillance in Singapore:
 - government inspectors / enforcement officers
 - SG Clean ambassadors
 - stories about kaypoh neighbours.
- Singapore has not seen the 'naming and shaming' that has occurred in some other countries.
- The Personal Data Protection Commission has taken care to emphasise the need to comply with the data protection law.

THANK YOU!

Lyn@lynboxall.com

William@straitsinteractive.com



DPEX

DATA PROTECTION EXCELLENCE NETWORK



Covid-19 and the Impact to Data Privacy Malaysia

Dr. Sonny Zulhuda

International Islamic University Malaysia & DPEX Network

sonny@iium.edu.my



Reality Check on 28th Day MCO

- Malaysia under Movement Control Order means: more online works, online meetings, online shopping, online learning and online games.
- Increased risk of security and data privacy breaches including scam, social engineering, malicious software, and data abuses.
- Malaysians are advised to be more vigilant and mindful of what they share online as well as other online activities.
- Among the biggest risk of PDPA breaches:
 1. Illicit requests of personal data for online services, Apps, etc;
 2. Unauthorised disclosure of personal information relating to Covid-19 patients or suspects;
 3. Unsecured online meetings that reveal personal data, confidential information or official secrets.

Health-related Issues under PDPA

- There is a general exemption on the processing of personal data by Federal and State Governments (s. 3(1))
- Sensitive personal data (section 4)
“any personal data consisting of information as to the physical or mental health or condition of a data subject...”
- The processing of “sensitive data” (section 40)
 - With explicit consent, or
 - Necessary processing, including to protect the vital interests of the data subject or another person.
 - Necessary for medical purposes by a healthcare professional or someone under confidentiality.
- “Medical purpose” includes the purposes of preventive medicine, medical diagnosis, medical research, rehabilitation and the provision of care and treatment and the management of healthcare services.
 - Mobile Apps on health assessment?
 - Plan of Apps on contract tracing?

UM researchers design digital thermometers that can collect real time data

NATION 

Thursday, 02 Apr 2020

By **CHRISTINA CHIN**



PETALING JAYA: Universiti Malaya's researchers have come up with the country's first infrared (IR) digital thermometer that can collect real time data.

The Internet of Things (IoT) innovation can be used to predict and detect Covid-19 hotspots in real time and it is expected to be ready for testing by next week.

The team led by Prof Dr Ng Kwan Hoong from the Faculty of Medicine and Assoc Prof Dr Nahrizul Adib Kadri from the Faculty of Engineering includes Assoc Prof Dr Yeong Chai Hong from Taylor's University and engineers Darween Reza Sabri and Ricky Liew from a local startup.

Govt launches pilot project to monitor spread of Covid-19 pandemic via app

MOBILE APPS

Monday, 06 Apr 2020

5:15 PM MYT

By Qishin Tariq



Tweet

Khairy Jamaluddin ✓
@Khairykj

Satu app juga sedang dibangunkan dengan segera bersama @kkmm_gov untuk memudahkan contact tracing terutamanya selepas PKP tamat. The app will enable @KKMPutrajaya to alert people who have been exposed to those infected with COVID-19, an important mitigation strategy post MCO.

3:29 PM · Mar 25, 2020 · Twitter for iPhone

1.3K Retweets 2K Likes

Partial Exemptions under section 45 of the PDPA 2010

- Personal data processed **in relation to information of the physical or mental health of a data subject** shall be exempted from the **Access Principle** and other related provisions of this Act of which the application of the provisions to the data subject would be likely to cause serious harm to the physical or mental health of the data subject or any other individual;
- Personal processed **for preparing statistics or carrying out research** shall be exempted from the **General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle** and other related provisions of this Act, provided that such personal data is not processed for any other purpose and that the **resulting statistics or the results of the research are not made available in a form which identifies the data subject**;
- Also some partial exemptions apply on the **discharging of regulatory functions and journalistic purposes**.

Other Concerns and Conclusion

- The involvement of a 3rd party as service provider will make him as a data processor under the PDPA. Their role and duties may trigger the application of some provisions under the PDPA, especially under Security, Disclosure as well as Retention issues.
- Privacy policies on those initiatives will need to be notified and publicised to achieve transparency and to ensure due diligence.
- Any initiatives that help to control or reduce the spread of Covid-19 would be warmly welcome by the Malaysians, but being mindful of the privacy concerns is still needed as privacy is not only a matter of PDPA compliance but also a common law rights for individuals.

THANK YOU!



Dr. Sonny Zulhuda
International Islamic University Malaysia &
DPEX Network



sonny@iium.edu.my



Question & Answer

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

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

William Hioe – Singapore (FIP, CIPP/E, CIPP/A, CIPM, CIPT, GRCP)

Jon Bello – Philippines (FIP, CIPP/E, CIPM)

Dr Prapanpong Khumon – Thailand

Dr Sonny – Malaysia

TraceTogether Review

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

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



TraceTogether

Review Methodology

- Global Privacy Enforcement Privacy Sweep Study – Mobile Applications
- Application of the 9 Obligations of Singapore’s Personal Data Protection Act (PDPA)
- Application of the Generation Data Protection Regulation (GDPR) principles – *(available in research paper)*

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.

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 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.

Benchmarking the TraceTogether app against the GPEN survey parameters

In 2014 GPEN 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

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.

Use of Permissions

Dangerous permissions used in TraceTogether

Dangerous: Photos/Media/ Files	<ul style="list-style-type: none"> • read the contents of your USB storage • modify or delete the contents of your USB storage
Dangerous: Storage	<ul style="list-style-type: none"> • read the contents of your USB storage • modify or delete the contents of your USB storage
Dangerous: Location	<ul style="list-style-type: none"> • approximate location (network-based) • precise location (GPS and network-based)
<u>Normal</u>	<ul style="list-style-type: none"> • receive data from Internet • access Bluetooth settings • full network access • prevent device from sleeping • view network connections • pair with Bluetooth devices • run at <u>startup</u>

Permission Group	Permissions
CALENDAR	<ul style="list-style-type: none"> • READ_CALENDAR • WRITE_CALENDAR
CAMERA	<ul style="list-style-type: none"> • CAMERA
CONTACTS	<ul style="list-style-type: none"> • READ_CONTACTS • WRITE_CONTACTS • GET_ACCOUNTS
LOCATION	<ul style="list-style-type: none"> • ACCESS_FINE_LOCATION • ACCESS_COARSE_LOCATION
MICROPHONE	<ul style="list-style-type: none"> • RECORD_AUDIO
PHONE	<ul style="list-style-type: none"> • READ_PHONE_STATE • CALL_PHONE • READ_CALL_LOG • WRITE_CALL_LOG • ADD_VOICEMAIL • USE_SIP • PROCESS_OUTGOING_CALLS
SENSORS	<ul style="list-style-type: none"> • BODY_SENSORS
SMS	<ul style="list-style-type: none"> • SEND_SMS • RECEIVE_SMS • READ_SMS • RECEIVE_WAP_PUSH • RECEIVE_MMS
STORAGE	<ul style="list-style-type: none"> • READ_EXTERNAL_STORAGE • WRITE_EXTERNAL_STORAGE

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.’

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)

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.

Reviewing the TraceTogether App against the Nine Obligations in the PDPA

Consent & Notice Obligation

1. When downloading the TraceTogether app and setting it up so that it will work, the user needs to provide consent for 'push notifications'.
 - to be alerted for contact tracing purposes or, once contact tracing ceases, to prompt the user to disable the app.
 - **This is not mentioned in the privacy statement** for the TraceTogether app; nor is it explained clearly in the accompanying materials
 - It is assumed that individuals downloading the app will understand why they are consenting to push notifications.

Reviewing the TraceTogether App against the Nine Obligations in the PDPA

Consent & Notice Obligation

2. When **downloading** the TraceTogether app and setting it up so that it will work, the user needs to provide consent for the app to track the location of the mobile phone.

- Permission is necessary in an Android phone so that the Bluetooth technology will work. The app does not collect or store location information.

Reviewing the TraceTogether App against the Nine Obligations in the PDPA

Consent & Notice Obligation

3. When **downloading** the TraceTogether app and setting it up so that it will work, the user needs to turn on the Bluetooth function on their phone

In summary, the user is notified of the purposes for which the TraceTogether app will collect 'close proximity' information and gives consent to it exchanging information with other mobile phones running the TraceTogether app in order for the app to do so.

Reviewing the TraceTogether App against the Nine Obligations in the PDPA

Consent & Notice Obligation

The TrackTogether app's privacy statement says:

- 'With your consent, [the app] 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.'
- 'When you are close to another phone running TraceTogether, both phones use Bluetooth to exchange a Temporary ID



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.

I want to help



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.

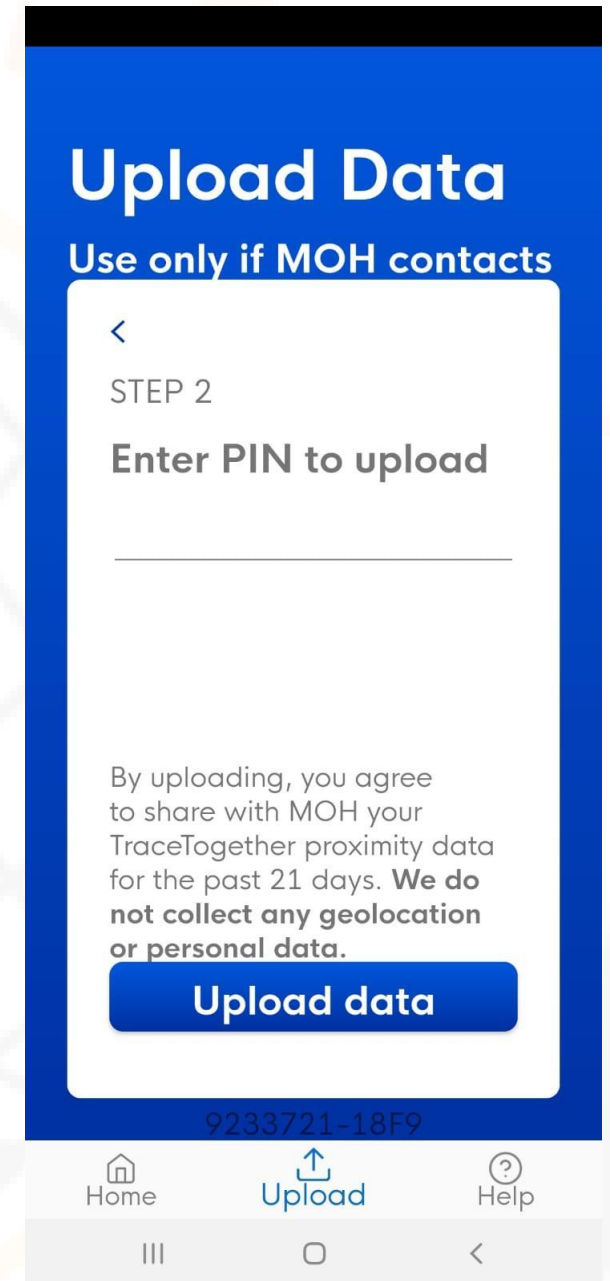
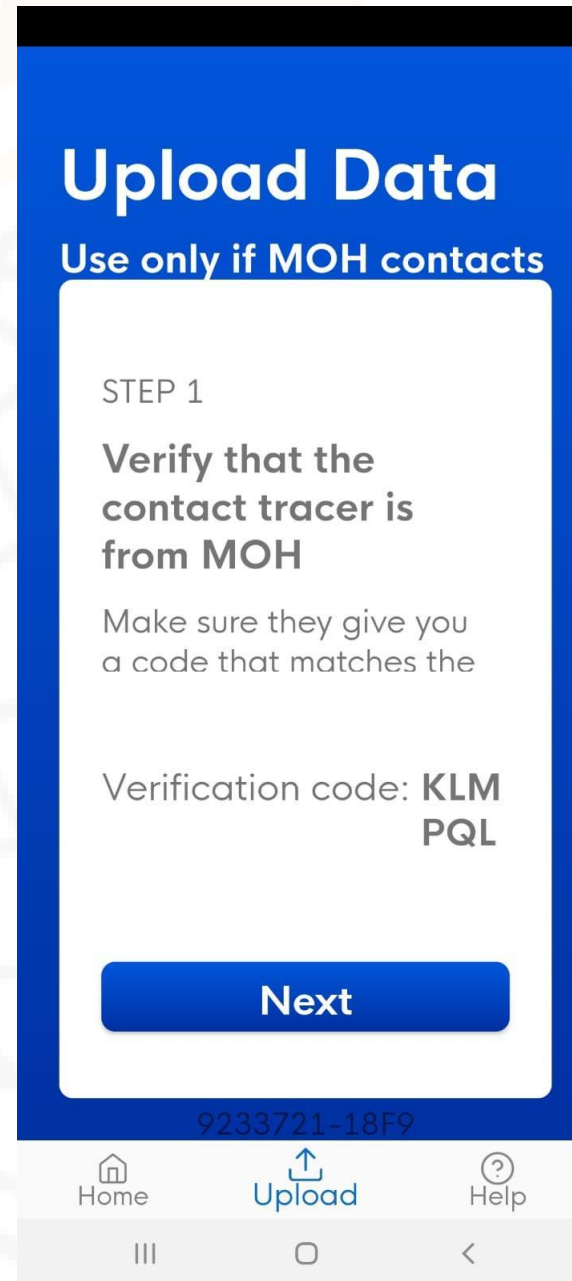
Great!!!

Reviewing the TraceTogether App against the Nine Obligations in the PDPA

- Consent & Notice Obligation

4. After the user has downloaded the TraceTogether app and used it they may be contacted for contact tracing purposes.

Conclusion: GovTech and MOH have complied with the consent obligation and the notification obligation in each of these four situations, albeit with a minor reservation regarding consent for 'push notifications'.



Reviewing the TraceTogether App against the Nine Obligations in the PDPA

Excessive Collection of Personal Data

- Our analysis of the privacy statement and the permissions sought by the TraceTogether app shows that it collects, uses and discloses personal data **only to ‘facilitate the contact tracing process’**.
- The app makes a very conscious effort to **collect only minimal information that is relevant to contact tracing**.
- Other than the mobile phone number, the app does not collect any other contact information whatsoever.

Conclusion: the app does not collect excessive personal data.

Reviewing the TraceTogether App against the Nine Obligations in the PDPA

Withdrawing Consent

The privacy statement for the TraceTogether app says that the consent to collect 'close proximity' information can be revoked at any time:

- 'You can revoke consent by emailing support@tracetgether.gov.sg with the mobile number you registered in the app.
- We will then delete your mobile number and User ID from our server. This renders meaningless all data that your phone has exchanged with other phones, because that data will no longer be associated with you.'

Conclusion: the app allows withdrawal of consent

Reviewing the TraceTogether App against the Nine Obligations in the PDPA

Purpose Limitation Obligation and Notification Obligation

- GovTech and MOH might have chosen to collect information about the specific location of users of the TraceTogether app when they were in 'close proximity' to an individual who is subsequently found to be infected with COVID-19.
 - information might have been useful, for example, in identifying and analysing clusters of infection.
- GovTech and MOH have taken care to restrict the collection, use or disclosure of personal data by the app to stated purposes.

Conclusion: the app **complies with Purpose Limitation Obligation**

Reviewing the TraceTogether App against the Nine Obligations in the PDPA

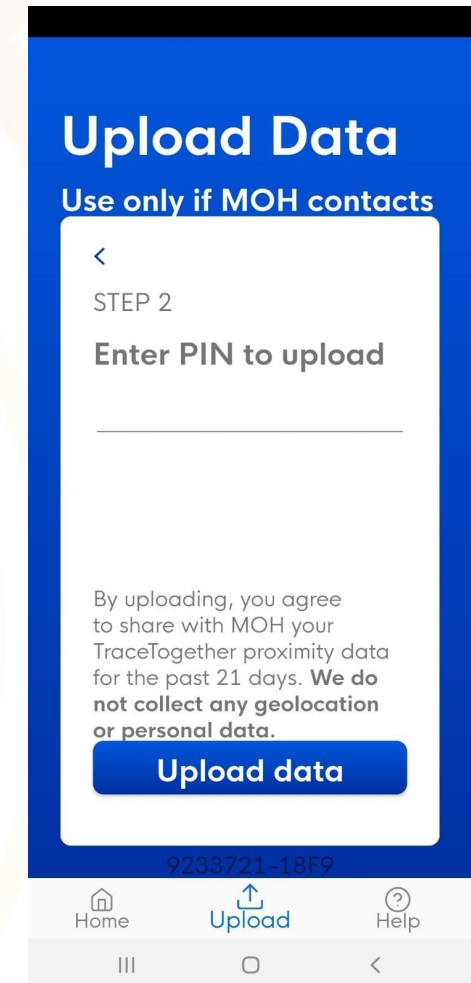
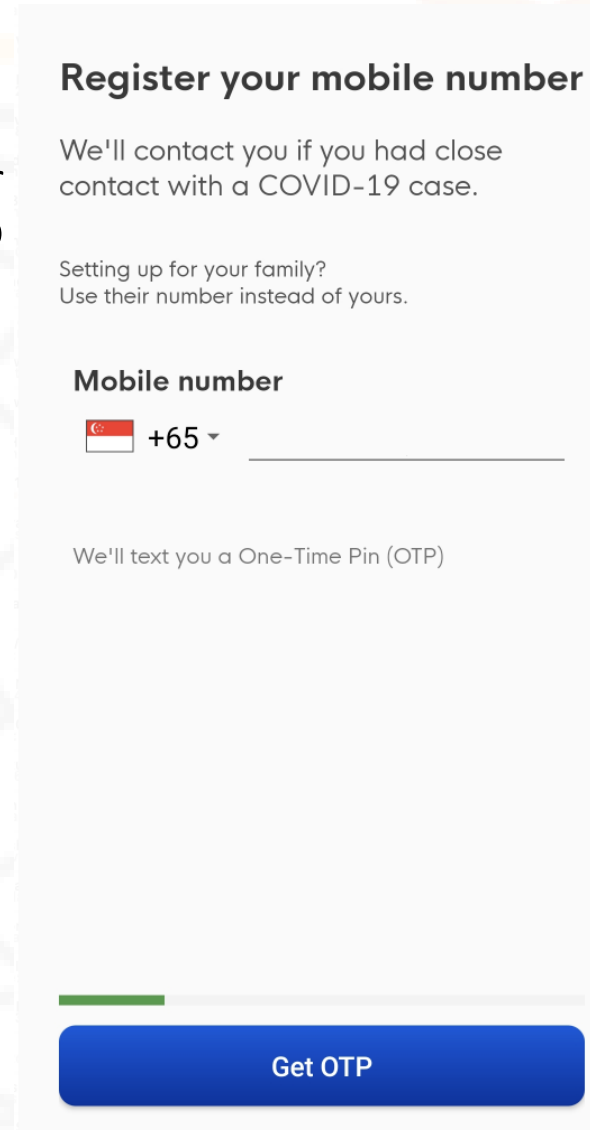
Access and Correction Obligation

- The TraceTogether app does not give an option for the user to obtain access to their personal data, to be told how it may have been used or disclosed within the previous year or to correct it.
- Unnecessary / Not relevant - the app only collects the mobile phone number

Accuracy Obligation

- The TraceTogether app verifies the user's mobile number with two-factor authentication using a One-Time Pin (OTP) sent to the mobile phone number provided by the user of the app:
 - During the registration process
 - When the user is asked to upload information) when contacted by MOH)

Conclusion: the app complies with the Accuracy Obligation



Reviewing the TraceTogether App against the Nine Obligations in the PDPA

Retention Limitation Obligation

- The user's mobile phone number will be retained by GovTech for as long as COVID-19 epidemic measures require contact tracing.
- This is supported by the privacy statement saying that:
 - "Once contact tracing ceases, you will be prompted to disable TraceTogether's functionality."
 - "You can revoke consent by emailing support@tracetogogether.gov.sg with the mobile number you registered in the app."
 - "We will then delete your mobile number and User ID from our server. This renders meaningless all data that your phone has exchanged with other phones, because that data will no longer be associated with you."
- The app documentation says 'close proximity' information is deleted on a rolling 21 days basis.

Conclusion: the app complies with the retention limitation obligation

Reviewing the TraceTogether App against the Nine Obligations in the PDPA

Retention Limitation Obligation

- The app documentation says that ‘close proximity’ information is deleted on a rolling 21 days basis
- Whether the code is written in such a way that the ‘close proximity’ information is automatically purged after 21 days (versus being archived) is unknown.
- In addition, the privacy statement says that:
 - ‘The Temporary ID ... is refreshed at regular intervals.’

In summary, GovTech will hold the mobile phone number of a user of the TraceTogether app until the user revokes their consent or disables the app.

Conclusion: it **seems** that GovTech and MOH have done everything possible in designing the app to ensure that personal data will not be retained when it is no longer necessary for contact tracing purposes.

Reviewing the TraceTogether App against the Nine Obligations in the PDPA

Transfer Limitation Obligation

- Not relevant

Accountability Obligation

Conclusion: The TraceTogether app satisfies both aspects of this final obligation, including through the information provided in the privacy statement and accompanying documents and in the way the TraceTogether app has been designed.

Summary

1. GPEN Benchmark: the types of permissions sought by the TraceTogether app do not exceed what would be expected based on the app's functionality and, with one exception, explains clearly why it wants specific information and what will be done with it.

The exception concerns location data permissions.

The developers could have proactively clarified potential confusion arising from a technical need to seek this permission against the practicality that location information is not collected or stored by the TraceTogether app.

Summary

2. The privacy statement and accompanying documents explain clearly and in simple English

- what the TraceTogether app does
- what kind of personal data is collected
- and how it may be used or disclosed

The permissions the app seeks *do not exceed* its functionality and declared purposes.

Summary

3. The TraceTogether app does not comply with all of the nine obligations under the PDPA, but is generally consistent with those obligations and principles.

The few areas where it falls short tend to reflect the nature of an app such as the TraceTogether app rather than an inadvertent or careless departure from an obligation.

CLOSING

THANK YOU!

