SK·CHAMBERS
ADVOCATES & SOLICITORS

CONTACT TRACING: BALANCING BETWEEN PANDEMIC AND PRIVACY

Does the COVID-19 pandemic allow data users to disclose personal data to the government?

SK Chambers – Thong Xin Lin

Introduction

The coronavirus disease (COVID-19) needs no further introduction. With close to 470,000 cases and 22,000 deaths reported to-date[1], governments worldwide have adopted drastic measures to curb the pandemic including imposition of lockdowns and travel bans, prohibition of mass gatherings and closing down of educational institutions.

Other interventionist (albeit necessary) steps that have been taken from the beginning of the outbreak include contact tracing – a process initiated to identify persons who may have come into contact with an infected person. Data plays an imperative role especially in contact tracing where information disclosed to the authorities is relied on to identify infected persons as well as other persons they may have been in contact with. In most cases, authorities require geolocation data and social contact history of an individual for the purpose of contact tracing.

Varying degree of data use in contact tracing

Having said that, the extent that data is used in contact tracing varies for each jurisdiction ranging from analysing anonymised datasets to disclosing details of the daily routines of the infected persons to the public. Examples:

(a) The United Kingdom (UK): The UK Information Commissioner's Officer (ICO) issued an official statement on 12 March 2020 clarifying, among others, that while it is unlikely that companies will be asked to share information about specific individuals with public authorities, data protection law would not prevent that.[2] In this regard, it is worth noting that the UK data protection law does not prevent the processing of personal data where it can be reasonably concluded that this is needed to protect individuals and the public generally, as the safety and security of the public remains the compelling public interest in the current health emergency.[3] For example, the law does not prevent the sending of public health alerts which are vital to the management of health risks and incidents such as COVID-19, nor does it prevent the use of technology to facilitate safe and speedy consultations and diagnoses.[4] However, if the situation in the UK worsens (e.g. if a state of emergency is declared), it is possible that more intrusive forms of data collection and processing may start to become justifiable.[5]

(b) Italy: Efforts have been initiated using anonymised datasets from Facebook and local telco companies to produce an aggregated and anonymised heatmap to help with contact tracing

and to enable authorities to better understand population movements in order to thwart the spread of COVID-19.[6]

(c) Singapore: The collection, use and disclosure of personal data without consent is permissible for the purpose of carrying out contact tracing and other response measures. An advisory was issued by the Singapore Personal Data Protection Commissioner on 13 March 2020 stating that in the event of a COVID-19 case, this is necessary to respond to an emergency that threatens the life, health or safety of other individuals.[7] Additionally, the Singapore government has launched a contact-tracing smartphone app to allow authorities to identify those who have been exposed to people infected with coronavirus as part of efforts to curb the spread of the disease.[8] The app will work by exchanging short distance Bluetooth signals between phones to detect other participating users in close proximity of two metres. Records of the encounters will be stored locally on each phone with the app, and if the need arises, this information can then be opted by the user to be disclosed to the Ministry of Health to identify close contacts based on the proximity and duration of an encounter between two users.[9] While downloading the app is not compulsory, the Singapore government is taking steps to encourage people to do so.[10]

(d) Israel: Israel passed an emergency law recently to use mobile phone geolocation data for tracking people with infected with COVID-19 to identify people they have come into contact with and may have infected, and to subsequently require the latter group of people to go into quarantine.[11]

(e) South Korea: South Korea's Infectious Disease Control and Prevention Act was previously amended in the aftermath of the Middle-East Respiratory Syndrome (MERS) outbreak to equip the government with extensive legal authority to collect private data as well as to disclose information to the public about the movement paths, transportation means and contacts of patients of the infectious disease.[12] In managing the COVID-19 outbreak, it was reported that the authority relied on closed-circuit television camera footage, credit card records and mobile phone Global Positioning System (GPS) data for verification and released details about patients' travel history via text messages on mobile phones and state-managed websites.[13] The government's efforts to boost transparency have since been met with criticisms due to the extreme level of detail of information being released which have reportedly exposed unwelcome details about individuals' private lives.

Disclosure for the purpose of contact tracing – permissible?

Data in the possession of entities and businesses may potentially be harnessed for the purpose of contact tracing and other measures. For example, social contact history of infected persons would be necessary to trace all persons whom the infected person has been in contact with. This, however, will need to be balanced with the existing data protection framework in Malaysia. In such circumstances, is it permissible for companies to disclose personal data in their possession to the authorities without the data subject's consent?

Generally, personal data under the Personal Data Protection Act 2010 (PDPA) is defined to mean any information in respect of commercial transactions that relates to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user. Therefore, data such as the name, National Registration Identity Card (NRIC) number and mobile number of an individual is personal data. Other information such as geolocation data and social contact history of a person where combined with other information in the

possession of a data user that is able to identify an individual will also be considered as personal data, in which case the PDPA applies.

It is worth emphasising that the obligations under the PDPA (including that personal data must not be disclosed without the consent of the data subject) are only applicable to the processing of personal data. Therefore, in a situation where the information that has been requested by the authorities is unable to identify any individuals, whether or not when considered with other information in the possession of the data user (e.g. anonymised datasets), such information does not amount to personal data and the obligations set out under the PDPA do not apply.

On the other hand, where the PDPA does apply, the data user is required to comply with the obligations under the PDPA. The main obligations under the PDPA involves obtaining the consent of and notifying the data subject for the processing of personal data being carried out by the data user. Personal data must generally not be disclosed without the consent of the data subject. The data user must also take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction, and must not keep personal data any longer than is necessary for the fulfilment of the purpose when it was first collected.

Having said that, where the request made by authorities is in fact in relation to personal data, the disclosure can still be made legally without contravening the PDPA. There are certain instances where disclosures are permitted under the PDPA. Disclosure for the purpose of contact tracing would likely fall within the following categories of permitted disclosures under the PDPA:

(a) <u>The disclosure was required or authorised by or under any law</u> (Section 39(b)(ii) of the PDPA)

If the disclosure is required or authorised to be made by a data user pursuant to a requirement set out under a law, such disclosure is permitted under the PDPA. The following are some examples of laws which can require disclosure of personal data to be made:

Applicable Law	Requirement
Communications and Multimedia Act 1998 (CMA), Section 263(2)	A licensee shall, upon written request by the Malaysian Communications and Multimedia Commission (MCMC) or any other authority, assist the MCMC or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence under any written law of Malaysia or otherwise in enforcing the laws of Malaysia, including, but not limited to, the protection of the public revenue and preservation of national security. Section 39(b)(ii) of the PDPA would be applicable where the request for assistance is made by an authority in relation to the provision of personal data that is in the possession of the data user.
Malaysian Aviation Commission Act 2015 (MACA), Section 81	The authorised officer may make an order against any person, among others, to give the authorised officer any information or to produce to the Malaysian Aviation Commission any such documents, if he has reasonable grounds to believe that that person: (a) has any information or any document that is relevant to the performance of functions and powers under the MACA; or (b) is capable of giving any evidence which the authorised

	officer has reasonable grounds to believe that the evidence is relevant to the performance of functions and powers under the MACA. Among others, the function of the Malaysian Aviation Commission is to provide a mechanism for the protection of consumers. Section 39(b)(ii) of the PDPA would be applicable where the request for information or documents is in relation to the provision of personal data that is in the possession of the data user.
Land Public Transport Act 2010 (LPTA), Section 232(1)	Every road transport officer making an investigation under the LPTA shall have the power to require information, whether orally or in writing, from any person supposed to be acquainted with the facts and circumstances of the case under investigation. Section 39(b)(ii) of the PDPA would be applicable where the request for information is in relation to the provision of personal data that is in the possession of the data user.

In particular, Section 263(2) of the CMA enables <u>any</u> authority to approach a licensee under the CMA and make a written request for such licensee to provide assistance as far as reasonably necessary in preventing the commission or attempted commission of an offence under any written law of Malaysia or otherwise in enforcing the laws of Malaysia.

It is worth noting that it is a criminal offence under the Prevention and Control of Infectious Diseases Act 1988 (PCIDA) for a person who knows or has reason to believe that he is suffering from an infectious disease to expose other persons to the risk of infection by his presence or conduct. In particular, Section 12(1) of the PCIDA reads as follows: "no person who knows or has reason to believe that he is suffering from an infectious disease shall expose other persons to the risk of infection by his presence or conduct in any public place or any other place used in common by persons other than the members of his own family or household".

Any authority can rely on Section 263(2) of the CMA to request the assistance of a licensee under the CMA, as far as reasonably necessary, to provide information including personal data such as the name, phone number and location touchpoints of individuals on the basis that such a request is to prevent the commission or attempted commission of an offence under Section 12(1) of the PCIDA.

(b) <u>The disclosure is necessary for the purpose of preventing or detecting a crime</u> (Section 39(b)(i) of the PDPA)

If the disclosure of personal data is necessary to prevent or detect a crime, such disclosure is permitted under the PDPA. For example, the Personal Data Protection Code of Practice for the Banking and Financial Sector provides that the disclosure of personal data is permissible pursuant to this sub-section where information regarding individuals suspected of fraud, or abetting the same, is disclosed to one or more data users in order to prevent and/or detect future attempts to defraud the data user.[14] Essentially, this sub-section can be relied on if a law provides that a certain conduct is considered a crime and such disclosure is permitted to prevent or detect such conduct.

Where an authority requires a data user to provide information for the purpose of contact tracing, any disclosure of personal data pursuant to such request would likely be a permitted disclosure pursuant to Section 39(b)(i) of the PDPA considering that the conduct of any person who knows or has reason to believe that he is suffering from an infectious disease exposing other persons to the risk of infection by his presence or conduct in any public place or any other place used in common by persons other than the members of his own family or household, is a criminal offence.

(c) The disclosure is necessary for the purpose of investigations (Section 39(b)(i) of the PDPA)

Even if there is no specific law or crime that can be pinpointed to for the purpose of disclosure, it would appear that the disclosure may still be made pursuant to the second limb of Section 39(b)(i) of the PDPA if the personal data is required for the purpose of an investigation. The term "investigation" has been construed widely enough, in several Personal Data Protection Codes of Practice issued by the Personal Data Protection Commissioner, to recognise the disclosure of personal data to a forensics specialist in an internal investigation[15] as well as disclosure to the police in the course of investigations[16].

Thus, any investigation carried out by the authorities for the purpose of contact tracing would arguably fall within this limb as well, and any disclosure of personal data to such authorities would likely be considered as a permitted disclosure under the PDPA.

Other obligations under the PDPA

Even if disclosure to authorities in the current circumstances are permissible, it is equally imperative for data users to ensure that steps are also taken to comply with the other obligations under the PDPA.

In particular:

(a) Security: Practical steps must be taken to protect personal data from, among others, any misuse, loss or unauthorised disclosure. If personal data is being disclosed to authorities, data users should consider whether there are sufficient measures in place to protect the personal data from any misuse, loss or unauthorised disclosure.

(b) Retention: Personal data disclosed to the authorities must not be retained for any longer than necessary for its purpose.

(c) Destruction: Once there is no longer any necessity for the personal data to be retained, such personal data must be destroyed or permanently deleted. Therefore, if the authorities require personal data for the purpose of contact tracing, such personal data that has been disclosed to the authorities for such purpose must be destroyed after the process for contact tracing has been completed.

Under the PDPA, the abovementioned obligations fall on the data user. Therefore, when such personal data is being disclosed to authorities, the data user should consider if such issues have been adequately addressed.

It is worth noting that the Personal Data Protection Code of Practice for several classes of data users including licensees under the CMA as well as the aviation and utilities sectors provide that in instances where requests for disclosures of personal data are directed to data users pursuant to a request of a regulatory or statutory authority, or where the disclosure is required or authorised by or under any law or by an order of court, data users are required to:

(a) only release the requested personal data on a formal written request being made, citing the relevant legal basis of the request being so made; and

(b) wherever appropriate, set conditions stipulating the permitted use of the personal data and its return or destruction upon the conclusion of the purpose of the requestor.[17]

Perhaps data users may consider imposing conditions to ensure that:

(a) Practical steps are taken to protect the personal data that has been disclosed to the authorities from any misuse, loss or unauthorised disclosure;

(b) Personal data that has been disclosed to the authorities will only be used for the purpose for which it was requested; and

(c) Upon the fulfilment of the purpose in which the personal data was requested by the authorities, such personal data must be destroyed or permanently deleted.

Key takeaway

Disclosure of personal data can be done for the purpose of contact tracing in Malaysia without eroding the existing data protection framework in place. Having said that, besides assessing the permissibility of such disclosures, it is equally crucial for data users to not neglect the other obligations it is required to comply with under the PDPA when disclosing personal data such as ensuring security of the personal data and the destruction of such personal data when its purpose has been served.

Footnotes

[1] https://www.worldometers.info/coronavirus/

[2] https://ico.org.uk/for-organisations/data-protection-and-coronavirus/

[3] https://www.withersworldwide.com/en-gb/insight/in-this-time-of-covid-19-does-personal-data-privacy-get-thrown-out-the-window

[4] https://www.withersworldwide.com/en-gb/insight/in-this-time-of-covid-19-does-personal-data-privacy-get-thrown-out-the-window

[5] https://www.withersworldwide.com/en-gb/insight/in-this-time-of-covid-19-does-personal-data-privacy-get-thrown-out-the-window

[6] https://privacyinternational.org/examples/3422/italy-telcos-turn-over-anonymised-location-data-aid-contact-tracing

[7] https://www.pdpc.gov.sg/Advisory-on-CUD-for-COVID-19

[8] https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether

[9] https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether

[10] https://www.thestar.com.my/business/business-news/2020/03/21/singapore-launches-contact-tracing-mobile-app-to-track-coronavirus-infections

[11] https://techcrunch.com/2020/03/18/israel-passes-emergency-law-to-use-mobile-data-for-covid-19-contact-tracing/

[12] https://www.lawfareblog.com/lessons-america-how-south-korean-authorities-used-law-fight-coronavirus

[13] https://www.straitstimes.com/asia/east-asia/how-china-s-korea-and-taiwan-are-using-tech-to-curb-outbreak

[14] Example 3 for Paragraph 3.3.6(ii) of the Personal Data Protection Code of Practice for the Banking and Financial Sector

[15] This was cited as an example in the Personal Data Protection Code of Practice for the Banking and Financial Sector, Personal Data Protection Code of Practice for the Utilities Sector and Personal Data Protection Code of Practice for the Aviation Sector

[16] This was cited as an example in the Personal Data Protection Code of Practice for the Banking and Financial Sector

[17] Paragraph 3.8 of the Personal Data Protection Code of Practice for the licensees under the CMA; Paragraph 2.63 of the Personal Data Protection Code of Practice for the Aviation Sector; Paragraph 2.4.4 of the Personal Data Protection Code for the Utilities Sector