# 4. Data privacy, security, and the future of data governance in Malaysia

*Moonyati Yatid and Farlina Said*

Throughout the course of the spread of COVID-19 in Malaysia, technology was deployed to control, investigate, and mitigate societal well-being beyond public health. Unmanned aerial vehicles like drones were used to monitor society's compliance with lockdown measures (Bernama 2020), e-commerce initiatives were rolled out under the government's economic recovery plan (MDEC 2020), and artificial intelligence-enabled thermal cameras were deployed (*New Straits Times* 2020). However, none of these was more contentious than the technologies used in contact tracing.

From the start of the pandemic, Malaysia introduced several contact-tracing applications driven by both federal and state initiatives. At the federal level, the three main applications were MySejahtera, MyTrace, and Gerak Malaysia. At the state level, there were SELangkah in Selangor and digital surveillance solutions in Sarawak. From August 2020, MySejahtera was mandatory for all business premises, with exemptions only for premises in rural areas or small towns without stable internet connectivity (*The Star* 2020).

In a landscape of evolving digital legislation, the swift implementation of such technologies could outpace efforts for data governance. Thus, the rapid adoption of these technologies could create vulnerabilities in the protection of privacy. As such, this chapter aims to cover the different technologies used in the mitigation of COVID-19 in 2020 with a focus on the contact-tracing applications that were developed. Subsequently, the chapter delves into data privacy and security concerns and concludes with reflections on Malaysia's technological future in data governance.

**How to cite this book chapter:**
Yatid, Moonyati; and Said, Farlina. 2022. 'Data privacy, security, and the future of data governance in Malaysia'. In: Shin, Hyun Bang; Mckenzie, Murray; and Oh, Do Young (eds) *COVID-19 in Southeast Asia*: *Insights for a post-pandemic world*. London: LSE Press, pp. 58–66. DOI: https://doi.org/10.31389/lsepress.cov.d

## Tech-less contact tracing and the efficacy of application-based contact tracing

Surveillance and public health in Malaysia were not initially so dependent on technology. The country's first case of COVID-19 was discovered on 25 January 2020 thanks to the Ministry of Health's Crisis Preparedness and Response Centre (CPRC) (Ahmad et al. 2020). Common procedures dictated that, from the diagnosis of a COVID-19 case, rapid assessment and rapid response teams would be deployed to collect the patient's socio-demographic information and travel and movement history over the previous 14 days. This established the patient's contact list for tracing (Ahmad et al. 2020). This tech-less contact tracing was the primary method used by the Ministry of Health (MOH) at that time, particularly for district health offices (Boo 2020).

To control rising infections, Malaysia's movement control order (MCO) was initiated on 18 March 2020. Malaysia's MCO had several iterations, corresponding with different standard operating procedures. The 18 March MCO was lifted and replaced by a recovery movement control order (RMCO) on 9 June 2020 in light of a decrease in the number of cases. Technology then began to be used, particularly to assess users' health and risk, to trace possible infections from a specific location, and as a means of delivering updated information and highlighting hotspots. As technology itself is transformative, throughout the MCO and the RMCO, contact-tracing applications in Malaysia learned from competing applications and modified their own processes.

Developers introduced several applications in the months between the MCO and RMCO. The applications differed in terms of ownership, methodology, privacy thresholds, and, where declared, data retention limits. To streamline efforts, an announcement on 3 August 2020 mandated that businesses owners and operators download and register with MySejahtera. With this announcement, and with MySejahtera being the only application tied to short-term economic plan (PENJANA) benefits, certain states such as Penang announced that they would phase out their own applications in favour of MySejahtera, thus consolidating contact-tracing applications into a centralised data collection system. The table below illustrates the different applications rolled out during the MCO; afterwards, PgCare and Gerak Malaysia ceased operation.

These applications had different practices for data retention and data protection. MyTrace, the development of which was led by the Ministry of Science, Technology and Innovation, used Bluetooth and anonymised

**Table 4.1. Contact-tracing applications used in various Malaysian states**

| Application | Developer | Function |
|---|---|---|
| MySejahtera | Federal government agencies (National Security Council [NSC], Ministry of Health [MOH], Malaysian Administrative Modernisation and Management Planning Unity [MAMPU], Malaysian Communications and Multimedia Commission [MCMC]) | Multi-purpose application intended for individuals to assess health levels, discover hotspots, seek health facilities, and receive latest updates and other materials from the MOH using web-based and QR-scanning functions |
| MyTrace | Federal government agencies (led by the Ministry of Science, Technology and Innovation [MOSTI]) | Bluetooth-enabled contact tracing, with data remaining anonymous and information about potential exposures stored only on one's device |
| SELangkah | Selangor state government | Location-based and QR code-enabled contact tracing |
| SabahTrace | Sabah state government | Location-based and QR code-enabled contact tracing |
| COVIDTRACE | Sarawak state government | Location-based and Bluetooth-enabled contact tracing |
| Gerak Malaysia (no longer in use as of 2021) | Federal government (MCMC and the Royal Malaysia Police [RMP]) | GPS-enabled contact tracing and QR codes to inform authorities of permissions granted to travel |
| PgCare (no longer in use as of 2021) | Penang state government | Location-based and QR code-enabled contact tracing |

data while retaining records of encounters on one's device. Sarawak's COVIDTrace also stated that user data would be anonymised, and geolocation data would not be collected. The information gathered by

COVIDTrace, Selangor's SELangkah, and Sabah's SabahTrace included the individual's name and phone number as well as the date and time of visits to relevant premises. SabahTrace also collected information on the user's body temperature.

MySejahtera is among the examples of centralised data collection tools for which data in transit was said to be encrypted. The data security and governance of MySejahtera were managed by the National Cyber Security Agency (NACSA), an arm of the National Security Council (NSC). Data retention limits for the applications ranged from 21 days to six months, though not all applications declared limits; MyTrace stated the duration of data retention in devices was 21 days (Bedi 2020), while MySejahtera's check-in feature retained data for 90 days (Krishnan 2020). The now-defunct Gerak Malaysia also stated that information on travel would be retained for six months after the MCO ceased. Meanwhile, COVIDTrace stated that, should users revoke consent, their data would be deleted from the system, thus protecting users from future data breaches.

While technology was crucial in mitigating infection rates, the efficacy of contact-tracing applications alone was questionable. For instance, only 4% of all reportedreports of COVID-19 cases in Malaysia were detected by MySejahtera (CodeBlue 2020). Researchers have highlighted, however, that contact tracing could work if it was part of a wider public health strategy and response that encompassed mass testing and strict physical distancing measures at the same time (Browne 2020). The self-assessment tool in MySejahtera detected positive cases with a success rate between 3.1% and 6.5% (Krishnan 2020). In addition, data gathered from the check-in function at a densely populated location could swiftly trace close contacts. A cluster at a large shopping complex resulted in the identification of 221 positive cases from 17,260 screened users, demonstrating an efficacy rate between 15.1% and 37.8% (Krishnan 2020). Such achievements justified the use of contact-tracing applications, as the MOH Director General, Dr Noor Hisham, attested in October 2020 (Palansamy 2020).

## Data privacy and security concerns

Privacy has diverse cultural interpretations. Joseph Savirimuthu (2016) has conceptualised privacy through the lenses of jurisdiction, space, and identifiable data. Such concepts were only nascent in Malaysia during the pandemic. Ipsos, a marketing research and consulting firm, surveyed Malaysians in 2019 and revealed a high degree of acceptance

of sharing data with the private sector or the government if there was a reward of better services or other benefits (Ipsos 2019). As 'data is the new oil', however, it could be tempting for companies and countries to abuse this receptivity for economic and political gains.

The multitude of applications available to Malaysians and low awareness about the management of data and privacy rights could lead to problems of mining digital platforms for information. In addition, increased surveillance and a culture of exchanging data for benefits could bear social and security-related consequences. Malaysia's data protection and privacy systems have had a poor reputation – in a 2019 study by Comparitech, Malaysia ranked fifth lowest out of 47 countries assessed (Tang 2020). Furthermore, Malaysia had previously suffered from serious data leaks, including the patient records of nearly 20,000 Malaysians (Habibu 2019) as well as 46.2 million mobile subscribers of Malaysian telecommunications companies and mobile virtual network operators (MVNO) (Vijandren 2017). With the Personal Data Protection Act (PDPA) of 2010 falling short of enforcing the mandatory reporting of data breaches, neither the severity of data breaches nor high cyber hygiene levels could be clearly assessed. Malaysia's data governance, however, could be judged by the capability of the government to protect users from data breaches and government efforts to construct standards upholding privacy.

First, heightened responsibility and accountability require appropriate legislation and enforcement. The PDPA possessed loopholes that weakened its protection of personal data beyond commercial purposes. This meant that the regulations did not include the government sector in its scope. While section 203A of the Penal Code provides penalties for any person who leaks information in the performance of their duties, the absence of mandatory data breach reporting rules for the private and public sectors reduced enforcement and transparency.

Additionally, the Act did not specifically address online privacy protections or users' privacy protections. Malaysia's challenges related to protecting privacy would require the reconciliation of cultural interpretations of privacy with technical possibilities. The notion of identity being separate from personal data was not a widespread practice, which could underlie the fundamental delay in the establishment of policy directions in data governance, as concepts and gaps in data classification needed time to become incorporated into policy and law. While international standards such as the EU General Data Protection Regulation (GDPR) had upheld user privacy by adding layers of protection such as

anonymisation, pseudonymisation, or encryption, Malaysia's laws and various personal data protection standards did not implement principles of data protection by design. This should be explored further as Malaysia's legislation on the matter develops.

Second, developing industry standards depends on the ability of the industry to uphold principles through various practices. An example of the different practices in security-by-design is the choice between centralised and decentralised data storage, each of which has different cybersecurity implications. The diversity of Malaysia's contact-tracing landscape indicated a variety of practices in data management. Contact-tracing applications in Malaysia utilised both centralised (MySejahtera and SELangkah) and decentralised (MyTrace and partial functions of COVIDTrace) models. MyTrace, for instance, utilised Bluetooth signals and proximity between devices to store information for contact tracing. Bluetooth signals are useful for data collection not directly associated with individuals, as the technology uses unique numbers in place of personally identifiable information. Additionally, MyTrace data was stored on users' devices for up to 21 days, which could assure users that their information was not shared or retained unnecessarily (Bedi 2020). Comparatively, MySejahtera collected data on a secured server with various details about users stored centrally. While MySejahtera's centralised database might have efficiently facilitated contact tracing for the MOH (Yusof 2020), the substantial amounts of information it collected could have unsettled users.

Through the lens of cybersecurity, both models have their weaknesses. For decentralised systems such as MyTrace, the security of the Bluetooth data collection depended on the application operator and the cyber hygiene of the user. In contrast, MySejahtera's centralised system meant that responsibility for data management was in the hands of a single body. Thus, while centralised databases can be more efficient, their weaker anonymity controls and data retention limitations can increase vulnerabilities when sharing information with the application.

As the PDPA and its lacking enforcement measures did not mainstream security-by-design conversations among developers, safeguards should be in place to protect users. Two ideas that can be considered are to collect the minimum data needed and to roll out deletion measures – either for the application or for the data itself. The right to forget should be discussed further in Malaysian social and legislative contexts such that information retained by any data collector can and should be deleted.

Learning from this experience, the government should also provide more transparency for its data processing – and other mechanisms of these applications – in order to gain more trust from citizens. There could also be platforms for citizens to provide open feedback to improve the applications. It is necessary for data to be retained for only a limited timeframe to serve only the specific purpose for which it was collected. In a nutshell, fully transparent and accountable privacy-preserving solutions should be embedded by design to balance the benefits and risks associated with personal data collection, processing, and sharing. Components of an awareness campaign should include channels to contact relative cybersecurity agencies for cybersecurity issues. Thus, the strategy should map out the responsibilities of respective cybersecurity agencies and provide avenues to possible assistance. Another campaign could make cyber hygiene a norm of cyber practices. As washing hands has become the norm to mitigate the risk of COVID-19, similar consistent reminders could relate to standard cyber hygiene practices such as updating applications frequently, reading terms and conditions before agreeing to anything online, being wary of personal information shared, and visiting sites that are secured with necessary certifications.

## Concluding reflections and anticipations for the future

The concerns surrounding the privacy and security aspects of technology, which was abruptly and extensively used to combat COVID-19, became more real as possibilities slowly began to look like reality. One example is the case of Singapore, which retracted its promise to safeguard the privacy of its official COVID-19 application users. In March 2020, when Singapore first introduced the TraceTogether application, the government repeatedly and explicitly vowed that the data collected would be used purely for contact-tracing purposes. Ten months later, however, after the application's use became mandatory, it was revealed that the data could also be accessed by police to conduct criminal investigations (Sato 2021). This aligns with warnings made by analysts about the dangers of technological tools being exploited and privacy and security being violated in efforts to heighten surveillance and control.

As with other countries, Malaysia also experienced an increase in technology use during COVID-19, which brought both positive and negative impacts to society. It is safe to say that technology will grow increasingly important in our daily lives, even beyond the pandemic. It is important to remember, however, that the issues of privacy and security should be prioritised: as the internet is borderless, no person,

organisation, or country is safe from the attacks of hackers with malicious intentions. While privacy and security concerns related to COVID-19 have largely been discussed in the context of contact-tracing applications, in the near future, other technologies such as vaccine passports could also pose a danger to privacy, particularly as sensitive data travels across borders. The damage of security and privacy violations would be unimaginable; hence Malaysia needs to take steps to protect its citizens at all costs. Transparency in the use of technology, especially in the processing of mass data, and creating platforms for open feedback from citizens, as well as other mechanisms that could instil trust from society, are among the first steps that should be considered. Further, although the political scene in Malaysia has been deemed unstable in recent times – with unpredictable and constantly changing leadership – joint efforts and unity in safeguarding citizens' privacy and security should be made a priority, regardless of who is in power.

## References

Ahmad, Noor Ani; Lin, Chong Zhuo; Rahman, Sunita Abd; bin Ghazali, Muhammad Haikal; Nadzari, Ezy Eriyani; Zakiman, Zazarida; Redzuan, Suziana; Taib, Salina Md; et al. (2020). 'First local transmission cluster of COVID-19 in Malaysia: Public health response'. *International Journal of Travel Medicine and Global Health*, vol. 8, no. 3, pp. 124–130. https://doi.org/10.34172/ijtmgh.2020.21

Bedi, Rashvinjeet S. (2020). 'Data from Covid-19 app MyTrace kept on phone, not govt servers, says Khairy'. *The Star*, 8 May. https://perma.cc/9QXN-MFB4

*Bernama*. (2020). 'COVID-19: MAF to use drones at 12 hotspots during MCO'. *Bernama*, 24 March. https://perma.cc/EPT7-A4ZX

Boo, Su-Lyn. (2020). 'How MySejahtera protects your data and does more than contact tracing'. *CodeBlue*, 12 August. https://perma.cc/P9L9-HG3T

Browne, Ryan. (2020). 'Why coronavirus contact-tracing apps aren't yet the "game changer" authorities hoped they'd be'. *CNBC*, 3 July. https://perma.cc/EG6J-QL5K

CodeBlue. (2020). 'MySejahtera directly tracked just 4% of Covid-19 cases'. *CodeBlue*, 18 November. https://perma.cc/SBK9-ZMY4 [Last accessed 20 May 2021].

Habibu, Sira. (2019). 'Health Ministry investigating leak of patient records'. *The Star*, 19 September. https://perma.cc/4AXM-AFQM [Last accessed 20 May 2021].

Ipsos. (2019). *Global Citizens and Data Privacy: A Malaysian Perspective*. https://perma.cc/5EXR-SH5B [Last accessed 20 May 2021].

Krishnan, Dhesegaan B. (2020). 'MySejahtera app helped Health Ministry detect 9,167 Covid-19 cases nationwide'. *New Straits Times*, 19 November. https://perma.cc/YV8E-3TSZ [Last accessed 20 May 2021].

Malaysia Digital Economy Corporation. (2020). *MDEC Rolls Out Micro and SMES E-commerce Campaign under PENJANA Recovery Plan*, 30 June. https://perma.cc/AP2J-X6VS [Last accessed 20 May 2021].

*New Straits Times*. (2020). 'TM unveils solution for Covid-19 early detection', 3 April. https://perma.cc/544H-XYHT [Last accessed 20 May 2021].

Palansamy, Yiswaree. (2020). 'Dr Noor Hisham: 1 Utama mall cluster in Selangor at sixth-generation infection'. *Malay Mail*, 20 October. https://perma.cc/4GG5-QBUA [Last accessed 20 May 2021].

Savirimuthu, Joseph. (2016). *Security and Privacy*, vol 3. UK: Routledge.

Sato, Mia. (2021). 'Singapore's police now have access to contact tracing data'. *MIT Technology Review*, 5 January. https://perma.cc/DK5H-NDUZ [Last accessed 20 May 2021].

Tang, Ashley. (2019). 'Study: Malaysia the fifth-worst country for personal data protection'. *The Star*, 16 October. https://perma.cc/49AW-5P9D [Last accessed 20 May 2021].

*The Star*. (2020). 'My Sejahtera App "a must for all businesses"', 4 August. https://perma.cc/A22G-3U2M [Last accessed 20 May 2021].

Vijandren. (2017). '46.2 million Malaysian mobile phone numbers leaked from 2014 data breach'. Lowyat.net, 30 October. https://perma.cc/UAS5-FE8R [Last accessed 20 May 2021].

Yusof, Teh Athira. (2020). 'MySejahtera app now mandatory for all business'. *New Straits Times*, 3 August. https://perma.cc/WZ82-23SM [Last accessed 20 May 2021].