# Chapter 4
# Smart City and Privacy Concerns During COVID-19: Lessons from Singapore, Malaysia, and Indonesia

**Melinda Martinus**

**Abstract** Although smart technologies for managing urban problems have gained traction in Southeast Asia, citizens, experts, and policymakers continue to express concerns over data protection and security. Smart technologies, such as big data, artificial intelligence, and the Internet of Things (IoT), are perceived as enablers for cities to control air pollution, reduce traffic, streamline public services, and make energy use more efficient. Yet experts underline that smart technologies' personal and behavioral data have not been adequately protected, thus bringing significant risk to individual privacy. However, the COVID-19 pandemic has further intensified the dialogue to address privacy concerns in the digital sphere. Drawing from the experience of COVID-19 tracing applications in Singapore, Malaysia, and Indonesia, this chapter finds that despite concerns about technical issues and accessibility, the practice of surveillance and the effectiveness of such technology adoption to fight COVID-19 remain in debate. The dialogue on data protection in the digital sphere has been more complex as there are contesting interests between the need to ensure public safety and the need to protect individual privacy.

## 4.1 Introduction

In recent years, the concept of the smart city has been gaining traction across cities around the globe. With many projections indicating that population growth in urban areas will only increase and cause further environmental-related challenges, many planners have proposed smart technology as a solution. Cities increasingly develop or adopt technology-led interventions such as big data, artificial intelligence, and the IoT to control urban problems, such as reducing air pollution and traffic, streamlining public services, and making energy use more efficient.

As a consequence of those interventions, urban citizens increasingly participate in those various digital platforms that further enable them to share their personal data

M. Martinus (✉)
ISEAS—Yusof Ishak Institute, 30 Heng Mui Keng Terrace, Singapore 119614, Singapore
e-mail: melinda_martinus@iseas.edu.sg

T. Phan and D. Damian (eds.), *Smart Cities in Asia*, SpringerBriefs in Geography,
https://doi.org/10.1007/978-981-19-1701-1_4

and behavior to technology providers. This intensive use of technology has exposed them to data breaches, cyberattacks, and possibly the threat of public surveillance.

This paper seeks to understand the risk of smart city adoption intruding on individual privacy. Using various cases of data breaches, cyberattacks, and the threat of public surveillance in Southeast Asia, this chapter highlights the nexus of development policy, politics, and dynamic risks coming from smart city adoption. This chapter further analyzes the issue of digital privacy concerns during the COVID-19 pandemic by looking specifically at the adoption of digital tracing applications' challenges and opportunities in Singapore, Indonesia, and Malaysia.

## 4.2 Smart Cities Development Context in Southeast Asia

Southeast Asia will undoubtedly soon be the fastest growing market for smart cities. Today almost 50% of the region's population lives in cities. It is estimated that the region will achieve 56% urbanization by 2030 (United Nations 2018).

The region is home to youthful, digitally savvy, and upwardly mobile populations (Sheng 2019). It has seen a dramatic increase in internet usage in the past years. Currently, 60% of the population has access to the internet, and this rate is higher in countries such as Brunei (95%), Singapore (89%), Malaysia (84%), Vietnam (59%), and Thailand (67%) (Ingram 2020). Digital sectors, mainly e-commerce, transport and food, online travel, digital media, and financial services, are predicted to unleash the region's maximum growth. Google, Singapore wealth fund Temasek, and consultancy firm Bain & Co (2020) highlight that six countries of the region, Singapore, Indonesia, Malaysia, the Philippines, Thailand, and Vietnam, are on track to unlock a $300 billion internet economy by 2025.

In light of urbanization and economic opportunities from the digital sector, the region has been increasingly pursuing smart city aspirations as a national development premise. Singapore, the pioneer of the smart city movement in the region, spearheaded the Smart Nation initiative in 2014, a program to harness digital technologies to empower the economy and improve public services that respond to Singapore's citizens' different and changing needs (Smart Nation Singapore nd).

Other countries in the region, particularly Indonesia and Malaysia, have also mobilized smart city strategies as a national plan. In 2017, Indonesia's Ministry of Communication and Information Technology Indonesia launched the 100 Smart Cities Movement to address urbanization issues and improve the quality of life of urban citizens. The program aims to work on six key areas: governance, people, economy, mobility, living, and environment. Similarly, Malaysia's government recently spearheaded the Malaysia Smart City Framework (MSCF) to present a national document to guide Malaysia's innovative city development across states and regions. The MSCF is strategically aligned with other domestic plans such as an urbanization policy, a physical plan, green technology, low-carbon cities, and Malaysia's global commitment to the New Urban Agenda (the UN-Habitat) and the Sustainable Development Goals (SDG) (Lim et al. 2020).

The Philippines introduced New Manila Bay, a 407-ha city and a new integrated central business district (CBD) enhanced by artificial intelligence. New Manila Bay is the biggest Belt and Road project between the Philippines and China to date and is estimated to be completed in 2030 (Seow 2017). Another new development, New Clark City, is the country's first new town development that integrates smart, green, and resilient solutions to address climate change and natural disasters.

Thailand's government plans to adopt a smart city approach to enhance investment in cities along the Eastern Economic Corridor (EEC), a special economic zone with a solid manufacturing base (Dunseith 2018). As the government of Thailand expects to generate US$43 billion for the realization of the EEC, the government has been enhancing four investment areas: improved infrastructure, business and industrial clustering, tourism, and new town development through smart urban planning.

The push for the adoption of smart cities for urban development has also become a regional movement in Southeast Asia. Initiated by Singapore during its Association of Southeast Asian Nations (ASEAN) chairmanship in 2018, the ASEAN Smart City Network (ASCN) was launched as a network of 26 pilot cities from all 10 ASEAN member states to work towards the common goal of smart and sustainable urban development. The network facilitates knowledge exchange and capacity building among the pilot cities and pairs them up with donors, solution providers, and the private sector. The network works on six service domains: civic and social, health and wellbeing, safety and security, quality environment, built infrastructure, and industry and innovation (Centre for Liveable Cities 2018). Some of the projects proposed by the pilot cities are e-health and telemedicine services for rural areas in Makassar, Indonesia; an integrated e-payment system in Singapore; converged command and control services for enhancing public safety in Davao, Philippines; and smart manufacturing and logistics in Chonburi, Thailand.

## 4.3 Smart City and Privacy Concerns

As smart cities have undoubtedly gained traction in the region, one concern emerging from their implementation is privacy, especially how service providers maintain integrity by protecting users' data. As the smart city facilitates interconnectivity between users and providers, data will be transferred and utilized through various processes, which often involves multiple parties communicating and gaining access to data (Braun et al. 2018). This complex interaction will certainly endanger users' privacy. The way information is managed and stored by authorities could also bring security threats, as it simultaneously links data with new sensors and systems of the latest smart technologies (van Zoonen 2016). Furthermore, data is stored and distributed across multiple devices, locations, and service providers, and this could, in turn, add complexities in managing an increased amount of personal data generated from smart applications (Rosadi et al. 2017). In Southeast Asia, data breaching concerns involving public services and smart technologies have appeared in several instances.

One landmark case is the data breach of the MyKad project in Malaysia. In 2001, the government of Malaysia launched a multipurpose national digital identity card as a validation tool and proof of citizenship other than the birth certificate. MyKad was projected to replace the old identity card—*Kad Pengenalan Bermutu Tinggi*—as a valid identity card for Malaysian citizens and permanent residents over 12 years old. As digitalization became a flagship national project and was predicted to help Malaysia achieve developed nation status, the MyKad project had become a critical national program (Thomas 2004).

When the government introduced the project, the people of Malaysia generally gave substantial support and showed enthusiasm for the program, as MyKad was intended to simplify four types of personal identity: the national identity card, driving license, passport application, and health information. The government of Malaysia set aside a RM 276 million budget (US$67 million) and selected the National Registration Department (NRD) as the lead government agency and several companies to expedite the implementation (Thomas 2004).

MyKad was developed as a converged identity card, where authorized Government Service Centres (GSCs) such as the NRD, the Road Transport Department, the Immigration Department, and the Royal Transport Department can read, write, print, and utilize specific information on the MyKad. The card is equipped with an intelligent chip and up-to-date biometric technology, such as a colored digital photograph and a digital scan of the cardholder's thumbprint in the chip. GSCs's mandate then includes front-to-end data management, which handles the application process, data storage, and communication with the database centers, which the NRD hosts.

As a result of this digital feature, the personal information in MyKad can be accessed by certain government agencies or selected third parties who have the appropriate access rights. Also, any grant of access rights to the various authorities and third parties have thus far been done administratively and without transparency or public disclosure (Thomas 2004). Another hurdle is that the *National Registration Act* 1959 and *National Registration Regulation* 1990 do not indicate explicitly what types of information or database access are restricted (Thomas 2004).

The issue of privacy in the MyKad case continued to attract public attention when the Malaysian government indicated that in the future, the card could facilitate online transactions such as the digital wallet, ATM access, and transit applications. Consequently, MyKad would not serve solely as a digital identity card but as a multipurpose card with considerable capacity for expansion to other domains (Thomas 2004). As such, data and privacy protection must be seriously addressed and standardized by regulations.

Another privacy issue in the smart city domain involves concerns over cyberattacks. Vendors of service providers usually deploy software and complex infrastructure for smart cities without sufficient cybersecurity standards; thus, when interacting with such equipment, users may be exposed to several hacks and malicious software variants (AlDairi and Tawalbeh 2017). The most common type of cybersecurity threats in smart cities are denial of service attacks, unauthorized network access, theft of personal information, online financial fraud, website defacement, application-layer attacks such as cross-site scripting, and penetration attacks (Bélanger and Carter 2008).

Cases of cyberattack and data breach appeared in the recent attack involving Indonesia's super app, Tokopedia. Tokopedia has been considered a champion of "shared economy" in the smart city era—along with the giant ride-hailing companies of Gojek and Grab—because its business model provides an e-commerce platform for small and medium enterprises (SMEs). With such a platform, individuals can now sell their goods and services by utilizing the internet and electronic devices. Tokopedia collaborates with various government services such as the State Electricity Company (PLN), the Municipal Waterworks (PDAM), and the National Gas Company to facilitate municipal services and payment subscriptions. Tokopedia's platform indeed revolutionizes municipal services as the super app helps increase accessibility and efficiency of government services in dealing with customers.

Currently, Tokopedia has more than 10 million sellers and 100 million active transactions every month. According to Tokopedia's website, 90% of the sellers enjoy the digital transactions provided by the super app. In order to participate in Tokopedia, customers must register using their mobile phone number or email address. Customers are invited to provide their valid address, date of birth, bank account, credit or debit card, or any information about their preferred payment. Customers also need to provide an identity card for verification. Consequently, they are releasing their essential personal data and financial information to enjoy services provided by Tokopedia.

In May 2020, Tokopedia confirmed that it experienced a single cyberattack that attempted to steal 15 million users' data from its super app (Eloksari 2020). The case had become the first and largest data leak involving the e-commerce sector in the country. In a statement to the Jakarta Post, a cybersecurity research group asserted that this cyberattack happened because Tokopedia has too many employees with access to the company's internal system (Eloksari 2020). Besides, many tech-companies that provide super apps like Tokopedia often rely heavily on third-party companies that integrate with their systems, which increases the vulnerability to hacking.

In response to customers' concerns, Tokopedia claimed that the cyberattack only attempted to steal data from its servers but assured customers that their passwords were still protected and no payment information had been leaked (Fachriansyah 2020). Customers were encouraged to change their password to ensure safety. However, some experts argued that although hackers did not steal password and payment information, some primary data that were hacked, such as phone numbers and email addresses, are also sensitive to cybercrime (Fachriansyah 2020). That information can further facilitate spam and phishing. Customers have the rights to data protection, and service providers must ensure that they are accountable.

In a similar sense, privacy and smart city issues also include concerns over freedom of personal space and threats of surveillance as the result of technology adoption. Unlike data breach threats and cyberattacks that threaten personal data, the threats of surveillance interface with people in public spaces in a direct way. People's privacy is exposed to an increasing degree as many cities have increasingly deployed hardware such as public cameras, traffic control, and facial-recognition tools to increase the city's responsiveness to crimes, vandalism, accidents, and many types of disruptions in public spaces.

Such technology deployment would not only perpetuate surveillance by authority but dramatically change the normative assumptions about society's conception of human behavior in public spaces (Graham 2002). It would be more common to embed opaque codes in computer systems in calculating exposure of risk of an individual. Further, surveillance technology would normalize certain behavior because governments, through their matrix calculation, now can draw a line between "acceptable" and "unacceptable" behavior (Graham 2002).

In the Philippines, the issue over privacy and public surveillance emerged when the Philippines' government introduced the Safe Philippines Project or the Safe PH Project—a flagship program led by the Department of the Interior and Local Government (DILG). The program aims to provide crime prevention measures by utilizing high-definition and advanced closed-circuit television (CCTV) to help authorities monitor the occurrence of crimes, identify perpetrators, and improve emergency response time (Caliwan 2019).

The project received unwavering support as crime has been touted as a critical problem in many cities in the Philippines. A government official claimed that the country could attain peace and order in the community and invite more investors to do businesses by improving safety and security in the public space. In one sense, this program will indeed sustain economic growth and jobs in the Philippines (Caliwan 2019).

However, the project was received with much resistance when President Duterte and President Xi Jinping of China called for a collaboration between Chinese technology providers (potentially Huawei) and local authorities in the Philippines (Mandhana 2019). The agreement confirmed a plan to provide 12,000 closed-circuit televisions and facial-recognition technology in Manila and Davao (Mandhana 2019). It remained unclear which Chinese technology provider would provide such hardware. However congressional opponents in the Philippines expressed concerns over the involvement of a third-party service provider from China, notably Huawei.

Huawei is best known to provide cutting-edge telecommunication technologies, especially mobile phones, 5G network equipment, and the IoT across the region. Their technology and low cost unarguably help many developing countries in achieving smart city aspirations. Nonetheless, over the years, Huawei's reputation got tarnished as many lawmakers and security-threat experts from Western countries increasingly conveyed concerns over its technology that could be exploited by the Chinese government, presenting a potentially grave national security risk (Lecher and Brandom 2019). Moreover, the Philippines and China's relationship is often troubled when it comes to strategic and political affairs. The two countries have long been in dispute over maritime boundaries in the South China Sea.

When asked about the concerns about Chinese technology, a senator from the Philippines asserted that if the Philippines' government wants to select vendors for critical infrastructure like closed-circuit television and facial-recognition technologies, it must not select Chinese vendors (Mandhana 2019). The case of concerns over third-party intrusions in the Philippines' surveillance system has underlined the importance of having standardized guidelines for selecting service vendors. As surveillance systems require high integrity in analyzing data gathered from hardware and potentially expose individuals' identity and behaviors in the public domain, the third-party vendors who provide the service must comply with regulations, particularly compliance with ethical procedures.

There is no doubt that the adoption of smart technology will bring with it risks to privacy. The cases of digital privacy intrusion in the form of data breaches, cyberattacks, and digital surveillance across Southeast Asia have become a public concern.

While policies to create a safety ecosystem are still being developed, the COVID-19 pandemic has completely altered the debate over this issue. To help to limit the spread of the coronavirus, policymakers suggest or even mandate the use of technology, for instance contact tracing applications. Users' participation in such technology use is encouraged despite there still being limited frameworks to shield privacy.

## 4.4 Public Safety and Privacy During COVID-19

The increasing adoption of various smart city technologies has undoubtedly brought personal data infringement concerns into the digital sphere. However, it was not until the COVID-19 pandemic loomed in the region that policymakers have given more attention to public safety and privacy, facilitated more dialogue, and intensified various efforts to improve laws and regulations in managing such challenges.

COVID-19 was declared a global pandemic by the World Health Organization (WHO) on 11 March 2020. As a measure to curb the spread of the virus, policymakers have utilized numerous digital technology measures, namely data monitoring systems, contact tracing, and health screening. Contract tracing, which has been widely deployed across the region, works to help health officials identify and track individuals who might have come into contact with an infected person. To do so, users must install the application on their mobile phones or wearables. The tracing application utilizes global positioning systems or Bluetooth devices on users' mobile phones, thus facilitating signal exchanges between phones.

The adoption of such measures requires voluntary participation from users. From the perspective of public safety, adopting such a technology helps health officials to act promptly. Users who are in close contact with people infected with COVID-19 will receive notification via the app, messages, and emails that they need to monitor their health condition. Other information such as quarantine guidelines, supportive services, testing, and clinical care services are also provided to assist users further to minimize the risk of transmission. Such measures are considered necessary as the COVID-19 vaccine has not yet been widely distributed at the time of writing this chapter.

However, the adoption of contact tracing is not without risks. To participate in the application, users must reveal their identity, such as an address, phone number, and household information, and also exchange their travel patterns, thus increasing personal data breach exposure. This issue has become a concern in the case of TraceTogether (Singapore), MySejahtera (Malaysia), and Peduli Lindungi (Indonesia).

### *4.4.1 Singapore: TraceTogether*

On 20 March 2020, Singapore's government released the TraceTogether application as a measure to enhance Singapore's contact tracing efforts. The app helps to more efficiently identify people who are in proximity to an infected person using the proximity data collected. Using Bluetooth technology, TraceTogether works by approximating the distance between users by measuring the strength of the signals received from other Bluetooth devices (tracetogether.gov.sg nd). This approximation further allows the application to calculate the length of communication between devices.

Although digital access is ubiquitous in Singapore, approximately 20% of its population is still underserved (Eigen and Gasser 2020). Hence, when the app was launched, it received criticism for not being accessible to those who do not possess a smartphone, especially the poor, the elderly, and children. These groups are also the ones who are the most susceptible to the virus. To make this application more accessible, the government introduced the TraceTogether token on 28 June and distributed it to 10,000 seniors (Eigen and Gasser 2020).

As of June 2020, three months after the app was introduced, the program received low participation from citizens. Less than a quarter of Singapore's population or only 1,800,000 people downloaded the application (Baharudin and Yip 2020). Meanwhile, to work properly, the application needs at least 75% of the population to use the app to increase density and allow more information exchange between mobile phones. When asked about this issue, Singapore's minister in charge of the Smart Nation Initiative pointed out that low participation was due to technical difficulties on iPhone or Apple devices (Baharudin 2020).

There was also a changing policy on ensuring compliance. When the application was introduced, participation was entirely voluntary. As an effort to increase participation among Singapore's residents, the government mandated the TraceTogether app or token be used at popular venues such as cinemas, workplaces, schools, and shopping malls. The government had also increased the number of tokens distributed to residents to encourage more participation (Wong 2020a).

In a statement, Singapore's education minister asserted that 70% adoption could help Singapore reach its next reopening level (Wong 2020a). However, this percentage of adoption can be achieved only through legal compulsion. The government will only get data from people who consent; however, if users do not consent, they could be prosecuted under Singapore's Infectious Disease Act (Ng 2020). The act mandates the public authorities in charge with the responsibility for regulation of diseases and disease control. Any action that could hinder or obstruct the public authority to do so could be an offense according to the Infectious Disease Act (Global-is-asian 2020).

The issue of privacy first appeared when nearly 40,000 people signed a petition highlighting the poor interoperability of the existing TraceTogether smartphone app across various brands of smartphones (Low, nd). Most importantly, the petition underlined concerns over the wearable device's (token) 24/7 surveillance. However, government officials responded to this false suspicion. TraceTogether would not allow contact tracers to locate a person's location based on their proximity to other users' devices because the token does not have GPS or internet connectivity (Global-is-asian 2020).

The government of Singapore stated that TraceTogether is different from a tracking device or an electronic tag. The government improved TraceTogether's privacy safeguards, such as storing data limited to mobile phone number, identification details, and user ID only. A user's personal information is stored on a secure server and never shown to the public. Users are allowed to request to delete data from the server. The government also ensured that third-party services would not access users' data. The tracking data stored in the personal devices will be stored no longer than 25 days according to the TraceTogether privacy safeguards. The evolution of TraceTogether's privacy safeguards shows that the Singaporean government acknowledged the strength of public attitudes and the importance of privacy and data protection concerns and sought to anticipate debates by building in some level of privacy protection (Goggin 2020).

The privacy safeguard design of TraceTogether was "fairly elegant" and "preserves a fair degree of privacy" (Goggin 2020). In several interviews, Singaporean government officials ensured that when the pandemic is over, people will get instructions to destroy their data to ensure safety. It is not surprising that TraceTogether received much praise for its innovation. Gartner, a market research firm, made TraceTogether the Asia–Pacific winner for its 2020 Government Eye on Innovation award based on a poll of government organizations worldwide (Wong 2020b). TraceTogether is not a silver bullet to curb the spread of the coronavirus, yet its ability to widely reach and consistently track possible close contacts should augment human contact-tracers' efforts (Asher 2020).

All the praise received by TraceTogether is not without challenges. Recently, TraceTogether came under fire after authorities disclosed that police used the data for a murder investigation—after the government released a statement that the application will only be used for COVID-19 containment (Tarabay 2021). After a public outcry, Singapore's parliament passed a bill restricting the use of personal contact tracing data to serious criminal investigations only (Chee 2021). Singapore's minister in charge of the Smart Nation Initiative stated that limiting the use of contact tracing data within the proposed law is "a result of a delicate balance between the right to public health, the right to public security, and respecting the sensitivity of personal data during this extraordinary time" (Chee 2021).

### 4.4.2 Malaysia: MySejahtera

In order to eliminate the spread of COVID-19, the Malaysian government launched MySejahtera, a centralized portal that allows residents to monitor their health and share it with the Ministry of Health. It consists of several features that include self-assessment, a COVID-19 hotspot map, statistics of COVID-19 cases, information on health facilities, and a QR code scan for checking in at the premises. Recently, the government also announced that the application can be used for vaccine registration (Yeoh 2021).

Although MySejahtera is developed by federal government agencies and is mandatory for all businesses in Malaysia, several states also developed their own QR-based contact tracing. These applications include those developed by SELangkah (Selangor), SabahTrace (Sabah), CovidIDtrace (Sarawak), and PgCare (Penang) (Said 2020). The contact tracing application in Malaysia is rather non-homogeneous, and several states demonstrated strong governance in their localities (Said 2020).

MySejahtera faced various technical difficulties. First, as the cases of COVID-19 reached four-figure increases daily in early 2021, the health officials became overwhelmed in facilitating help for suspected cases. Many people claimed they had not received assistance, although they had already filed a report to health officials. Although the app was supported widely by the federal government, the government still needed thousands of physical contact traces. At least 30 tracers per 100,000 were still required to free up existing health professionals (Sukumaran 2021). These physical contact tracers could consist of professional personnel or volunteers.

Second, there was a concern about external parties' involvement when the application was launched. According to its website, MySejahtera was developed by strategic cooperation between the National Security Council (NSC), the Ministry of Health (MOH), the Malaysian Administrative Modernization and Management Planning Unit (MAPU), the Malaysian Communications and Multimedia Commission (MCMC), and the Ministry of Science, Technology and Innovation (MOSTI). However, there is no clear information on whether the app was developed internally by the government agencies or whether any external vendor was involved in the development. MySejahtera failed to provide more details regarding this concern (FocusM 2020).

Among the concerns raised, the issue of privacy seems to be the most prominent one. To register in MySejahtera, users need to provide a great deal of personal information, such as contact number, email address, full name, identity card, age, gender, ethnicity, and home address. To operate fully, the application requires access to smartphones' cameras, Bluetooth, flashlight, and full internet network access. Personal data privacy has always been a big issue in Malaysia, as the country experienced several data breach cases in the digital sphere. One of the most recent ones was the leak of 46 million mobile phone numbers from mobile operators and various professional associations, affecting the entire country (BBC 2017).

A research report from the Asia Pacific Training Centre for Information and Communication Technology for Development (APCICT/ESCAP) also highlights that MySejatera has not yet stated how personal data is processed and offers little explanation on how permissions are being used in the app (APCICT/ESCAP 2020).

Digital security experts also raised a concern about the power balance between government control and citizens' rights to personal privacy. Although the application must adhere to the Personal Data Protection Act (PDPA) 2010—the national act that regulates the procession of personal data to comply with certain obligations—the government is not subject to the law. Under PPDPA 2010, the government is not accountable for any data leaks, cyberattacks, or other breaches due to negligence (OneTrust Data Guidance 2020).

Experts also raised concerns about the efficacy of MySejahtera if it is balanced against concerns of privacy and personal choice. For instance, although the government periodically stated that the application had helped the government to identify COVID-19 cases, the government did not clarify whether the cases were from people who were mandated to download the app from the voluntary download.

### *4.4.3 Indonesia: PeduliLindungi*

Like TraceTogether and MySejahtera, Indonesia launched PeduliLindungi in late March, 2020 to curb the spread of the coronavirus. The application, developed by the Ministry of Communications and Information and the Ministry of State-Owned Enterprises (SOEs), utilizes a Bluetooth connection to detect another user whose data has been uploaded to PerduliLindungi's servers. This detection could help enable the exchange of data. If a user is found near confirmed suspected cases, the application will prompt a notification.

There were some technical issues when the program was introduced. As of April 2020, the application was installed by a couple of million people, although Indonesia has more than 100 million smartphone users (Florene 2020). Meanwhile, to work properly, contact tracing apps need approximately three-quarters of the population to install the application. Experts indicate that this requirement is due to the application not providing much information (Florene 2020). The application only points out a risky zone without details about the risk and the number of cases in each area.

When the application was introduced, the privacy concern also quickly gained ground. A group of human rights organizations addressed an open letter to the Indonesian minister of communication and information technology, demanding more privacy safeguards. When the application was launched, no application privacy safeguard was stated under the App Store or Google Play. The experts also requested the government release the white paper and source code for the PeduliLindungi application, provide a clear privacy policy, issue data privacy regulations, provide information about a recent data breach, and take steps to protect the right to privacy (Jakarta Post 2020).

There is also a concern over the risk of malware in the use of the PeduliLindungi application. As the application requires users to keep activating their Bluetooth, there is a risk of a malware attack for those who do not regularly update their Bluetooth application (Wira 2020). In general, when users start their Bluetooth and pair their phone to another phone, they must receive a notification. However, there is no such feature for users who do not have the latest version of Bluetooth. Malware can steal confidential information stored in a phone, such as password and credit card details.

Constant surveillance by the government was also another concern, as the application constantly notifies users if they are in crowded areas or zones with many cases (APCICT/ESCAP 2020). There are no detailed explanations of the technicalities of data acquisition in the application, as it seemed to utilize both Bluetooth and geolocation at the same time. Unlike Singapore's TraceTogether application that uses a single Bluetooth tracing method without acquiring geolocation data, PeduliLindungi's application seems to be much riskier.

A report from the Citizen Lab, Munk School of Global Affairs, shows that Indonesia's PeduliLindungi might acquire too much unnecessary data, risking more personal privacy while having less effectivity in minimizing the spread of the virus (Lin et al. 2020). According to the report, the application collected a great deal of data, such as geolocation, permission to take photos and video, and permission to access users' storage to allow the application to read users' photos and files. These are unnecessary data as tracing applications need only to communicate with other devices when in proximity.

However, the biggest concern is the way geolocation data is collected and managed, according to the report. The government selected Telkom Indonesia's server to store the end-point data. Appointing a third-party provider to oversee data will only increase the risk of a data breach. Data such as users' geolocations, Wi-Fi Mac addresses, users' phone numbers, and users' full names are stored in the third-party server, although none of these is necessary for contact tracing (Lin et al. 2020). TraceTogether, instead, can maximize the use of Bluetooth to detect nearby devices, especially those who are COVID-19 positive and to identify crowded areas.

Although the Indonesian government specifically regulated the use of TraceTogether through two decrees, Indonesia, in general, is still lacking comprehensive privacy laws in the digital sphere. For instance, there is no specific law that regulates punitive measures for parties who initiate a data breach. The current regulation only contains administrative sanctions such as oral and written warnings, temporary suspensions, and mandated announcements on the mass media (Florene 2020).

The COVID-19 pandemic has indeed further intensified the dialogue to address privacy concerns in the digital sphere. How this issue continues to evolve and what kind of interventions will be developed are still too early to predict. But the pandemic raises the question of whether protecting privacy must be absolute or whether it can be flexible in a time of crisis. If it can be flexible, to what extent should governments or the appointed authorities gather and use public data for the public interest, for example, monitoring the spread of disease, protecting citizens' health, and keeping the social order? And most importantly, how can we balance the urgency of maintaining public safety with the needs of protecting individual privacy?

## 4.5 Conclusion

There are indeed contested interests between the need to ensure public safety from the pandemic and privacy infringement concerns. However, some governments across the region have realized that there are increasing public concerns about privacy protection in the digital sphere. Most importantly, the case of contact tracing adoption across the region has indicated that many governments are demonstrating some efforts in building trust, namely improving written privacy safeguards and more transparency on the way users' data is managed, accessed, and stored. There are few things to take note of.

First, lawmakers must be clear in defining to what extent the law on privacy protection prevails above other laws. In Singapore's case, for instance, the law on privacy protection was adjusted in order to comply with any legal obligations, such as criminal law and laws on infectious disease. This adjustment will help the regulators and the public be better informed when there is a need to compromise the risk of privacy for public safety.

Second, there must be clear punitive measures for every stakeholder involved in data breaches. Privacy protection law must better state punishments for those who breach the laws without exception. As a preventive measure, if possible, law must limit the stakeholders involved in data processing and storing.

Third, as smart city adoption is becoming more complex and will involve many stakeholders in the future, there is a need to build more complex data protection layering. Regulators could oblige service providers by designing multiple components of data processing, so that there is a better opportunity to break attempts to breach data.

## References

AlDairi A, Tawalbeh L (2017) Cyber security attacks on smart cities and associated mobile technologies. Procedia Comput Sci 109:1086–1091. https://doi.org/10.1016/j.procs.2017.05.391

APCICT/ESCAP (2020) Resource materials on "data privacy laws in Asia and the Pacific." UNAPCICT. https://www.unapcict.org/resources/publications/resource-materials-data-privacy-laws-asia-and-pacific

Asher (2020) TraceTogether: Singapore turns to wearable contact-tracing Covid tech. BBC News

Baharudin H (2020) Wearable device for Covid-19 contact tracing to be rolled out soon, may be issued to everyone in Singapore, Politics News & Top Stories—The Straits Times. The Straits Times

Baharudin H, Yip WY (2020) Coronavirus: 25% of TraceTogether users update app to latest version. The Straits Times

BBC (2017) Malaysian data breach sees 46 million phone numbers leaked. https://www.bbc.com/news/technology-41816953. Accessed 5 Apr 2021

Bélanger F, Carter L (2008) Trust and risk in e-government adoption. J Strateg Inf Syst 17:165–176. https://doi.org/10.1016/j.jsis.2007.12.002

Braun T, Fung BCM, Iqbal F, Shah B (2018) Security and privacy challenges in smart cities. Sustain Cities Soc 39:499–507. https://doi.org/10.1016/j.scs.2018.02.039

Caliwan CL (2019) DILG launches "safe PH project" in Marikina. https://www.pna.gov.ph/articles/1086797. Accessed 5 Apr 2021

Centre for Liveable Cities (2018) ASEAN smart cities network. Singapore

Chee K (2021) Bill limiting police use of TraceTogether data to serious crimes passed. Politics News & Top Stories—The Straits Times. The Straits Times

Dunseith B (2018) Thailand's eastern economic corridor—what you need to know. ASEAN Business News. https://www.aseanbriefing.com/news/thailand-eastern-economic-corridor/. Accessed 5 Apr 2021

Eigen M, Gasser U (2020) Country spotlight: Singapore's TraceTogether program. https://cyber.harvard.edu/story/2020-07/country-spotlight-singapores-tracetogether-program. Accessed 5 Apr 2021

Eloksari EA (2020) Tokopedia data breach exposes vulnerability of personal data. The Jakarta Post. https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html. Accessed 5 Apr 2021

Fachriansyah R (2020) Data breach jeopardizes more than 15 million Tokopedia users, report finds. The Jakarta Post. https://www.thejakartapost.com/news/2020/05/03/data-breach-jeopardizes-more-than-15-million-tokopedia-users-report-finds.html. Accessed 5 Apr 2021

Florene U (2020) Indonesians skeptical of the state's COVID-19 prevention apps. KrASIA

FocusM (2020) MySejahtera privacy, safety concerns remain unaddressed. Focus Malaysia. https://focusmalaysia.my/mainstream/mysejahtera-privacy-safety-concerns-remain-unaddressed/. Accessed 5 Apr 2021

Global-is-asian (2020) Public health or privacy concern? The debate over contact-tracing apps. Global Is Asian. https://lkyspp.nus.edu.sg/gia/video/public-health-or-privacy-concern-the-debate-over-contact-tracing-apps. Accessed 5 Apr 2021

Goggin G (2020) COVID-19 apps in Singapore and Australia: reimagining healthy nations with digital technology. Media Int Aust 177:61–75. https://doi.org/10.1177/1329878X20949770

Google, Temasek, Bain & Company (2020) e-Conomy SEA 2020. https://www.bain.com/insights/e-conomy-sea-2020/

Graham S (2002) CCTV: the stealthy emergence of a fifth utility? Plan Theory Pract 3:237–241. https://doi.org/10.1080/14649350220150116

Ingram G (2020) Development in Southeast Asia: opportunities for donor collaboration. The digital world. Center for Sustainable Development at Brookings

Jakarta Post (2020) Human rights groups urge privacy protection in COVID-19 contact tracing efforts. The Jakarta Post

Lecher C, Brandom R (2019) Is Huawei a security threat? Seven experts weigh in. The Verge. https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g. Accessed 5 Apr 2021

Lim SB, Abdul Malek J, Hussain M, Tahir Z (2020) Malaysia smart city framework: a trusted framework for shaping smart Malaysian Citizenship? Handbook of Smart Cities. Springer. pp 1–24. https://link.springer.com/referenceworkentry/10.1007%2F978-3-030-15145-4_34-1

Lin P, Knockel J, Poetranto I et al (2020) Unmasked II: an analysis of Indonesia and the Philippines' government-launched COVID-19 Apps. Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto. https://citizenlab.ca/2020/12/unmasked-ii-an-analysis-of-indonesia-and-the-philippines-government-launched-covid-19-apps/

Low W (nd) Sign the petition. Change.org. https://www.change.org/p/singapore-government-singapore-says-no-to-wearable-devices-for-covid-19-contact-tracing. Accessed 5 Apr 2021

Mandhana N (2019) Huawei's video surveillance business hits snag in Philippines. Wall Street Journal

Ng A (2020) Coronavirus pandemic changes how your privacy is protected. CNET

OneTrust Data Guidance (2020) Malaysia—data protection overview. DataGuidance. https://www.dataguidance.com/notes/malaysia-data-protection-overview. Accessed 5 Apr 2021

Rosadi SD, Suhardi, Kristyan SA (2017) Privacy challenges in the application of smart city in Indonesia. In: 2017 international conference on information technology systems and innovation (ICITSI), pp 405–409

Said (2020) From the ground up: Malaysia's digital space amidst a pandemic. LSE Southeast Asia Blog. https://blogs.lse.ac.uk/seac/2020/11/16/from-the-ground-up-malaysias-digital-space-amidst-a-pandemic/. Accessed 5 Apr 2021

Seow J (2017) Manila's new smart city run by artificial intelligence. https://www.indesignlive.sg/projects/manilas-new-smart-city-run-artificial-intelligence. Accessed 5 Apr 2021

Sheng A (2019) Why Asean holds the edge in a digital future: it's the youth factor. South China Morning Post

Smart Nation Singapore Transforming Singapore (nd) Default. https://www.smartnation.gov.sg/why-Smart-Nation/transforming-singapore. Accessed 5 Apr 2021

Sukumaran T (2021) Why Malaysia's contact-tracing efforts are falling dangerously short. South China Morning Post

Tarabay J (2021) Countries vowed to restrict use of COVID-19 data. For one government, the temptation was too great. Fortune

Thomas M (2004) Is Malaysia's MyKad the "one card to rule them all"? the urgent need to develop a proper legal framework for the protection of personal information in Malaysia. Social Science Research Network, Rochester, NY

tracetogether.gov.sg (nd) TraceTogether privacy safeguards. https://www.tracetogether.gov.sg. Accessed 5 Apr 2021

United Nations (2018) The World's Cities in 2018

van Zoonen L (2016) Privacy concerns in smart cities. Gov Inf Q 33:472–480. https://doi.org/10.1016/j.giq.2016.06.004

Wira NN (2020) What to know before using PeduliLindungi surveillance app, according to cybersecurity expert. The Jakarta Post

Wong L (2020a) TraceTogether programme wins international award for innovative use of tech. The Straits Times

Wong L (2020b) TraceTogether check-ins to be compulsory at public venues in S'pore by end-December. The Straits Times. https://www.straitstimes.com/singapore/checking-in-with-tracetogether-to-be-compulsory-at-public-venues-by-december. Accessed 5 Apr 2021

Yeoh A (2021) MySejahtera now shows vaccine registration progress. The Star: Malaysia News