KHAZANAH
RESEARCH
INSTITUTE

Privacy and Cybersecurity:
Protecting Personal Data

VIEWS 41/20 | 1 October 2020 | Chua Shenyi and Rachel Gong

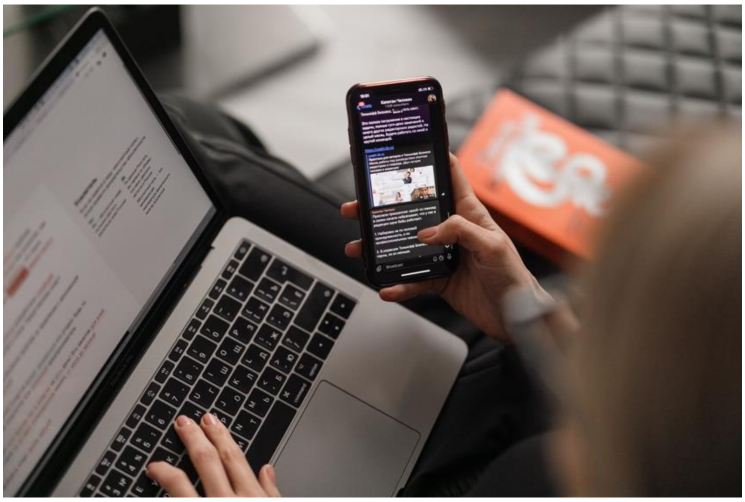
Views are short opinion pieces by the author(s) to encourage the exchange of ideas on current issues. They may not necessarily represent the official views of KRI. All errors remain the authors' own.

This view was prepared by Chua Shenyi and Rachel Gong, a researcher from the Khazanah Research Institute (KRI). The authors are grateful for valuable comments from Ahmad Ashraf Ahmad Shaharudin, Muhammad Nazhan Kamaruzuki, Amos Tong, Rueben Ananthan Santhana Dass, and Mary Beth Altier.

Corresponding author's email address:
rachel.gong@krinstitute.org

Information on Khazanah Research Institute publications and digital products can be found at www.KRInstitute.org.

Cover photo by Maxim Ilyahov on Unsplash.



Introduction

Increasing cases of massive personal data breaches suggest that Malaysians are at high risk of being the targets of scams. Police reports indicate that Malaysia loses an average of RM2 billion to scammers annually and that scammers possess accurate personal information of their targets[1]. A 2017 data breach in Malaysia leaked the personal details, including home addresses and myKad numbers, of about 46.2 million mobile number subscribers nationwide[2]. In April 2020, a 60-year-old hospital consultant from Pahang was scammed RM63,435 from his savings account shortly after sharing his online banking creditials on a fraudulent Bank Negara Malaysia website[3].

[1] The Star (2019)
[2] Tan and Sharmila Nair (2017)
[3] Pathma Subramaniam (2020)

Furthermore, ChannelNewsAsia reported that over 20,000 private medical records of Malaysian patients were published online and could be freely accessed by any internet user worldwide[4]. There has been concern that insurance companies may analyze leaked medical records and personal data to identify health risks and raise premium rates[5]. Individuals could also face workplace discrimination due to their medical histories, which may reveal, for example, depression or pregnancy[6]. It is clear that personal information should be properly protected and its use properly regulated.

Privacy is a fundamental human right recognized in the Universal Declaration of Human Rights of the United Nations[7] and "information privacy" is defined as "the right to select what personal information about me is known to what people"[8]. Despite recognising the value of privacy, internet users may be unaware of just how much of their personal data is being shared, to whom, and for what purposes.

In this article, we explore the question of privacy and security in a smartphone-enabled, data-driven world, specifically the risks associated with increased sharing of personal data, and suggest some ways individual users can protect their personal data.

What is personal data?

There are four types of consumer data that businesses collect: personal data, engagement data, behavioural data and attitudinal data[9]. In this article, we limit our discussion to personal data.

Personal data refers to any data that contains personally identifiable information. Malaysia's Personal Data Protection Act 2010 (Act 709) defines personal data as "any information…that relates directly or indirectly to a data subject, who is *identified* or *identifiable* from that information…"[10]; Singapore's Personal Data Protection Act 2012 defines it as "…data, whether true or not, about an individual who can be *identified* from that data…"[11]; The European Commission defines it as "any information that relates to an *identified* or *identifiable* living individual"[12] whereas the National Institute of Standards and Technology (NIST) of United States defines it as "information about specific individual…[that] can be used to *identify* the people who provided it"[13].

[4] ChannelNewsAsia (2019)
[5] Hart (2018); Allen (2018)
[6] Véliz (2019)
[7] United Nations (1948)
[8] Petrescu and Krishen (2018)
[9] Freedman (2020)
[10] Government of Malaysia (2010)
[11] Government of Singapore (2012)
[12] The European Commission (n.d.)
[13] Chad Boutin (2020)

The European Union's General Data Protection Regulation (GDPR) lists some examples of personal data including name, national identification number, location data, and even Internet protocol (IP) addresses that identify how a user is connecting to the internet[14].

Why are apps collecting personal data?

The COVID-19 pandemic has accelerated Malaysia's transition to a cashless society. Financial institutions and e-wallet service providers reported a steep rise in the transaction volume of contactless payments and e-wallet adoption during the movement control order (MCO) as Malaysians try to minimize physical contact. For instance, the sign-up rate for Maybank's MAE wallet doubled since the beginning of MCO[15] and the bank also expected a 30% growth in its eDuit Raya transaction volume for Hari Raya celebration this year[16]. Hong Leong Bank also witnessed a 13 fold increase in the total transnational value of e-wallet top-ups in two months from March to May 2020, as compared to the same period last year[17].

Similarly, two popular e-wallets in Malaysia reported growth in their number of users and transactions. GrabPay Malaysia has seen a 60% increase in new users with more than 8,000 new merchants signing up to use its digital service[18] and its contactless transactions have increased 1.7 times since the implementation of MCO[19]. Additionally, Touch 'n Go's eWallet saw an increase in e-wallet adoption among merchants[20] as well as a surge in e-commerce volumes and online transactions[21] during the MCO period.

Transitioning to the digital economy results in more people being more connected to the internet. Internet users share personal information with mobile applications or businesses in exchange for ostensibly free goods or services. Not only is money stored in e-wallets operated by private companies, but shared real-time location and personal information are stored in their databases too.

Smartphone apps can track our movements (e.g. whether we are sitting down or walking around), record our location, and read (some) text messages without any additional user action or input[22]. Businesses process these data into useful information that helps them provide better user experiences and services to their customers. For example, an individual uses an e-wallet to pay for a flight planned via a travel app and receives a confirmation email, including personally identifying information such as name, travel dates, locations, and payment details. These details are shared across multiple apps to automatically generate an event with details of the flight in the calendar of the user's smartphone.

[14] The European Commission (n.d.)
[15] The Star (2020)
[16] Ibid.
[17] Hong Leong Bank (2020)
[18] Boey (2020)
[19] The Star (2020)
[20] Birruntha (2020)
[21] Boey (2020)
[22] Ng and Kent (2018); Valentino-DeVries et al. (2018)

What are the risks of sharing personal data?

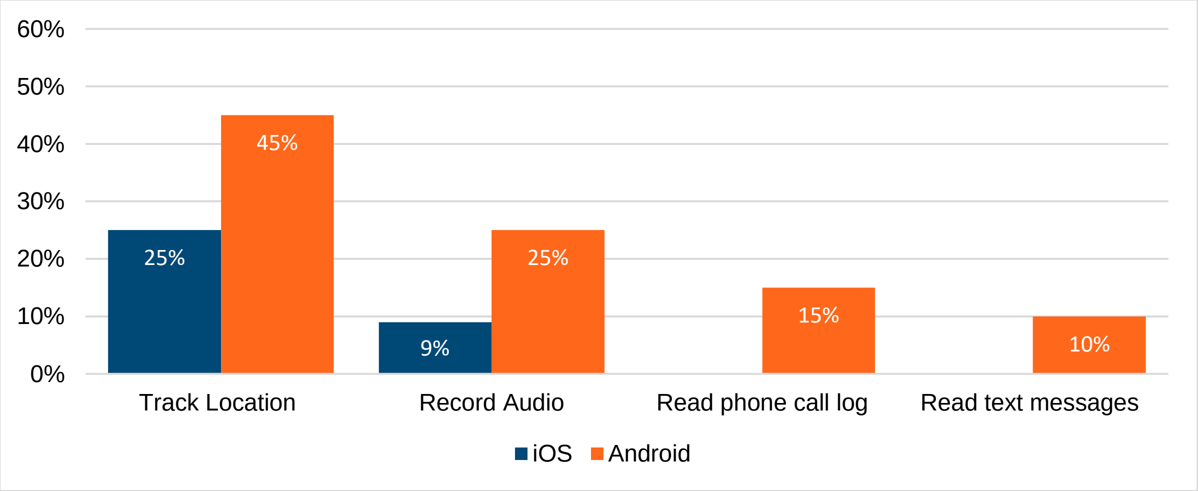
Despite the fact that personal data contains personally identifiable information, some might argue that "I have nothing to hide therefore I have nothing to fear", but the misuse of personal data can have unpleasant unintended consequences. Ride-sharing apps collect geolocation data to protect their drivers and passengers, but Uber's location data ended up being exploited by its employees to stalk politicians, celebrities and ex-partners[23]. Fitness app Strava includes a feature intended to enable runners to connect and build community, but the degree of personal data shared makes it easy to find out where a Strava user lives and what routes they usually run[24].

Apps are collecting more data than they actually need

A 2018 analysis by Symantec of the top 100 free mobile apps in Android and Apple iOS revealed that 89% of the apps on Android and 39% of the apps on Apple's iOS requested risky permissions. Risky permissions refer to "permissions where the app requests data or resources that involve the user's private information or could potentially affect the user's stored data or the operation of other apps". Some of the examples categorized as risky permissions by the study include access to location tracking, camera, audio recording, phone logs, calendar, contacts and SMS messages[25].

It was reported that Android apps requested more risky permissions compared to iOS apps (Figure 1): 45% of the Android apps analyzed requested access to track user location whereas only 25% of the iOS apps requested location access and 25% of the Android apps requested access to record audio while only 9% of the iOS apps requested similar access. Moreover, 15% of Android apps sought permissions to access text messages and 10% asked to access phone call logs. In contrast, such permissions are not accessible by iOS apps.

Figure 0: Breakdown of the risky permissions requested by the apps on each OS (%)



Note: Permissions to read phone call log and read text messages are not accessible by iOS apps
Source: Cleary 2018

[23] Gong and Chiam (2019)
[24] Seward (2020).
[25] Cleary (2018)

It is not clear that all these permissions are necessary for the apps to function properly. For example, a flashlight app on the Android OS sought permissions to access users' location services, contacts, text messages, microphone for audio recording purposes and even permissions to make phone calls or to reroute outgoing calls. Symantec stressed that users should be mindful of the permissions they grant each app, putting the burden on the end user when it should perhaps be placed on app developers by prohibiting the requirement of unnecessary permissions.

Oversharing personal data puts users at risk not only of potential stalking and attempts to manipulate their behaviour[26], but also of their personal information being added to a database that may not be adequately secured and thus may be susceptible to hackers and data breaches. Such breaches put them at further risk of identity theft and scams.

What can individual users do to protect personal data?

Securing a database from cybersecurity threats is out of the control of individual users so, until holistic data protection legislation is passed, individuals are best served by learning about the risks of data sharing and taking steps to minimise those risks.

In addition to **reviewing app permissions and evaluating whether the degree of personal data sharing is worth the benefits of the app**, we suggest two more ways individual users can protect their personal data.

Be aware of phishing attacks; verify requests for personal data

Phishing is a type of online scam often used to steal personal information such as login credentials, bank account information or credit card numbers[27]. Phishing attacks can occur through any form of communication, such as emails, phone calls, text messages, instant messages received on social media sites or advertisements[28]. Phishing messages typically claim to come from a legitimate source such as a bank or a government agency. Not only will phishers use the email address, logo and other trademarks from the purported source to look authentic, they will also fabricate stories to panic message recipients into either giving away personal data or allowing their personal data to be tracked. Examples of phising attacks include claiming a suspicious login attempt or unauthorized changes to the user's account have been detected or requesting confirmation to verify sensitive personal information[29].

According to the Malaysian Communications and Multimedia Commission (MCMC), the majority of the phishing attacks detected in Malaysia targeted internet banking users to trick them into revealing their login credentials[30].

[26] Zuboff (2019)
[27] MCMC (2020b); University of Massachusetts Amherst (n.d.)
[28] Ibid.
[29] MCMC (2020a)
[30] MCMC (2020b)

Cybersecurity Malaysia (CSM) also reported receiving a total of 838 cases involving fraud, intrusion and cyber-harassment in the early states of the MCO between March 18 and April 7[31]. Cybercriminals are quick in reacting towards global events, leveraging the pandemic to launch COVID-19 themed phishing emails or fraudulent websites filled with fake COVID-19 news[32] .

Before sharing any information, internet users should take additional steps to confirm who is requesting their personal data and for what purpose. For example, users receiving a text message about an unexpected financial transaction should contact their bank's customer service department to verify the message before responding to it. Users should also avoid clicking on links from suspicious emails without first verifying their source[33]. Fraudulent websites look very similar to original websites, differing by only a letter or punctuation mark. Examples include changing the letter O to the number 0 or inserting additional characters and symbols that legitimate web addresses will not have[34].

Be aware of social media settings; limit access to personal data

Social media users tend to unknowingly overshare personal information on these platforms, whether checking in at a restaurant for a meal, tweeting about a new job promotion or sharing photos with location details in the background or in the photo geolocation tag. While these activities are meant to foster meaningful connections with friends and family, there are privacy risks to such online sharing activities.

Social media posts uploaded on the internet may include personal details that malicious actors could exploit to access sensitive accounts or commit identity theft. Background information such as schools attended, pet names or vacation photos could provide enough clues for cybercriminals to work out a user's passwords[35].

Internet users should review privacy settings on their social media accounts to limit who can access their personal information. For example, on Facebook, users may want to avoid setting their posts to be public as that allows even non-Facebook users to access their information. Users may also want to consider reviewing their friend/follower list regularly to remove unfamiliar accounts that might be monitoring their posts.

Conclusion

Considering that personal data can be – and has been – misused when it falls into the wrong hands, there are several critical data governance questions we need to ask in this rapidly digitalising world: Who has access to our personal data? Where and how is our personal data being used and stored? What are the laws and regulations in place governing the access, use and storage of our personal data?

[31] Yuen (2020)

[32] Ibid.

[33] U.S. Federal Trade Commission (2012)

[34] Strawbridge (2018)

[35] Cybersecurity Malaysia (n.d.)

The responsibility of strengthening cybersecurity fall on the shoulders of all parties. It requires the efforts of both public and private sectors to coordinate and collaborate with each other in terms of capacity building and policy design and implementation.

As technology evolves and advances, the government could consider regularly reviewing and revising its existing regulations on personal data protection to ensure that data collected are secure and well-managed. Currently, the Personal Data Protection Act (PDPA) 2010 only protects inappropriate use of personal data for commercial purposes and the act does not apply to personal data processed outside of Malaysia[36]. Additionally, there is no Data Breach Notification Rule in the PDPA 2010 yet so businesses that suffer a data breach are not legally obliged to notify the authorities, the public, or the victims of the data leak[37].

Existing data protection laws also lack provisions to address children's digital privacy, personal data processed a) in non-commercial transactions and b) outside of Malaysia, as well as general online privacy issues such as geolocation data and browser cookies that could potentially track internet users[38].

Malaysia still has significant room for improvement in terms of cybersecurity and data protection. When the government takes the lead in data protection efforts through the introduction and strict enforcement of regulations, the private sector and the general public will slowly but surely follow.

[36] Naufal Fauzi (2019)
[37] Tashny Sukumaran (2019)
[38] Darmain Segaran (2020); Naufal Fauzi (2019)

References

Allen, Marshall. 2018. “Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates.” *ProPublica* (blog). July 17, 2018. https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

Birruntha, S. 2020. “E-Wallet Adoption on the Rise during MCO.” The Malaysian Reserve. May 21, 2020. https://themalaysianreserve.com/2020/05/21/e-wallet-adoption-on-the-rise-during-mco/.

Boey, Elaine. 2020. “Finance - Digital Payments Give Users More Bang for Their Ringgit.” The Edge Markets. August 16, 2020. http://www.theedgemarkets.com/article/finance-digital-payments-give-users-more-bang-their-ringgit.

Chad Boutin. 2020. “NIST Releases Version 1.0 of Privacy Framework.” NIST. January 16, 2020. https://www.nist.gov/news-events/news/2020/01/nist-releases-version-10-privacy-framework.

ChannelNewsAsia. 2019. “Almost 20,000 Medical Records of Malaysian Patients Found to Be Freely Available Online,” September 18, 2019. https://www.channelnewsasia.com/news/asia/malaysia-medical-records-patients-freely-available-online-11917748.

Cleary, Gillian. 2018. “Mobile Privacy: What Do Your Apps Know About You?” Symantec. August 16, 2018. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/mobile-privacy-apps.

Cybersecurity Malaysia. n.d. “Keep Yourself Safe from Online Identity Theft.” Accessed September 3, 2020. https://www.cybersecurity.my/data/content_files/11/763.pdf.

Darmain Segaran. 2020. “Child Digital Privacy in Malaysia: Risks, Regulation and Solutions.” *Dataraxis* (blog). January 7, 2020. https://www.dataraxis.co/blog-1/child-digital-privacy-in-malaysia-risks-regulation-and-solutions.

Freedman, Max. 2020. “How and Why Businesses Collect Your Personal Data (and What They’re Doing with It).” Business News Daily. June 17, 2020. https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

Gong, Rachel, and Hui San Chiam. 2019. “Personal Data Privacy and Surveillance Capitalism.” Khazanah Research Institute.

Government of Malaysia. 2010. “Personal Data Protection Act 2010 (Act 709).” http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20709%2014%206%202016.pdf.

Government of Singapore. 2012. “Personal Data Protection Act 2012.” December 7, 2012. https://sso.agc.gov.sg/Act/PDPA2012.

Harsha S, Khalid Nazim S A, S Balaji, and Vallabh V Rao. 2019. “Improving Wi-Fi Security against Evil Twin Attack Using Light Weight Machine Learning Application.” *COMPUSOFT: An International Journal of Advanced Computer Technology*, March. https://www.researchgate.net/publication/332344245_Improving_Wi-Fi_security_against_evil_twin_attack_using_light_weight_machine_learning_application.

Hart, Robert David. 2018. “Don’t Share Your Health Data with Insurance Companies Just for the Perks.” *Quartz* (blog). September 9, 2018. https://qz.com/1367202/dont-share-your-health-data-with-insurance-companies-just-for-the-perks/.

Hong Leong Bank. 2020. “Hong Leong Bank Introduces HLB Pocket Connect.” August 17, 2020. https://www.hlb.com.my/en/personal-banking/news-updates/hlb-introduces-hlb-pocket-connect.html.

MCMC. 2020a. “Identify Phishing E-Mail.” September 21, 2020. https://www.mcmc.gov.my/en/faqs/phishing-attack/2-identify-phishing-e-mail.

———. 2020b. “What Is Phishing?” September 21, 2020. https://www.mcmc.gov.my/en/faqs/phishing-attack/1-what-is-phishing.

Naufal Fauzi. 2019. “Data Privacy Laws: Malaysia Has a Long Way to Go.” *ISIS* (blog). February 12, 2019. https://www.isis.org.my/2019/02/12/data-privacy-laws-malaysia-has-a-long-way-to-go/.

Ng, Vivian, and Catherine Kent. 2018. “Smartphone Data Tracking Is More than Creepy – Here’s Why You Should Be Worried.” Yahoo! Finance. February 7, 2018. https://ca.finance.yahoo.com/news/smartphone-data-tracking-more-creepy-104117812.html.

Pathma Subramaniam. 2020. “TheWall: Protect Yourself against Covid-19 Scams.” The Edge Markets. May 25, 2020. http://www.theedgemarkets.com/article/thewall-protect-yourself-against-covid19-scams.

Petrescu, Maria, and Anjala S. Krishen. 2018. “Analyzing the Analytics: Data Privacy Concerns.” *Journal of Marketing Analytics* 6 (2):41–43. https://doi.org/10.1057/s41270-018-0034-x.

Seward, Andrew. 2020. Twitter Post. https://twitter.com/MrAndrew/status/1305530276127428609.

Strawbridge, Geraldine. 2018. “5 Ways to Identify a Phishing Website.” MetaCompliance. July 2, 2018. https://www.metacompliance.com/blog/5-ways-to-identify-a-phishing-website/.

Tan, Royce, and Sharmila Nair. 2017. “M’sia Sees Biggest Mobile Data Breach.” *The Star*, October 31, 2017. https://www.thestar.com.my/news/nation/2017/10/31/msia-sees-biggest-mobile-data-breach-over-46-million-subscribed-numbers-at-risk-from-scam-attacks-an/.

Tashny Sukumaran. 2019. “Malindo Air Confirms Data Breach, Exposing Records of Millions of Passengers.” *South China Morning Post*, September 18, 2019, sec. News. https://www.scmp.com/news/asia/southeast-asia/article/3027780/malindo-air-confirms-data-breach-exposing-millions.

The European Commission. n.d. “What Is Personal Data?” Accessed September 4, 2020. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en.

The Star. 2019. “Cops: RM2bil Lost to Scams,” August 8, 2019. https://www.thestar.com.my/news/nation/2019/08/08/cops-rm2bil-lost-to-scams.

———. 2020a. “Covid-19 Outbreak Steepens Adoption Curve of e-Wallets in Malaysia,” April 28, 2020. https://www.thestar.com.my/news/regional/2020/04/28/covid-19-outbreak-steepens-adoption-curve-of-e-wallets-in-malaysia.

———. 2020b. “Maybank Sees 30% Increase in EDuit Raya Transactions,” May 18, 2020, sec. Banking. https://www.thestar.com.my/business/business-news/2020/05/18/maybank-sees-30-increase-in-eduit-raya-transactions.

United Nations. 1948. “Universal Declaration of Human Rights.” December 10, 1948. https://www.un.org/en/universal-declaration-human-rights/.

University of Massachusetts Amherst. n.d. “Phishing: Fraudulent Emails, Text Messages, Phone Calls & Social Media.” Accessed September 21, 2020. https://www.umass.edu/it/security/phishing-fraudulent-emails-text-messages-phone-calls.

U.S. Federal Trade Commission. 2012. “How to Keep Your Personal Information Secure.” Consumer Information. July 2012. https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure.

Valentino-DeVries, Jennifer, Natasha Singer, Michael H. Keller, and Aaron Krolik. 2018. “Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret.” *The New York Times*, December 10, 2018, sec. Business. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

Véliz, Carissa. 2019. “Medical Privacy and Big Data: A Further Reason in Favour of Public Universal Health-Care Coverage.” In *Philosophical Foundations of Medical Law*, by Carissa Véliz, 306–19. Oxford University Press. https://doi.org/10.1093/oso/9780198796558.003.0022.

Yuen, Meikeng. 2020. “Cybersecurity Cases Rise by 82.5%.” The Star. April 12, 2020. https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity-cases-rise-by-825.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Public Affairs.