REVISITING THE RIGHT TO PRIVACY IN THE DIGITAL AGE: A QUEST TO STRENGTHEN THE MALAYSIAN DATA PROTECTION REGIME

Md Toriqul Islam*, Abu Bakar Munir** and Mohammad Ershadul Karim***

Abstract

The world goes through diverse privacy dilemmas, particularly after the discovery of Information Communication Technologies (ICTs) in the 1960s. It can be argued that such a scenario will continue in the future, as the vast majority of our works are done online using personal data. Perceivably, in the future, our online activities will increase, being facilitated by the pace, efficiency, accuracy of borderless connectivity and commercial engagement of the ICTs. Invariably, we are being captured on cameras, monitored and identified by numerous public and private actors, and all these lead to threats to our privacy. There is no one-size-fits-all solution to privacy problems due to the inefficiency of the regulatory measures and the pace of the growth of ICTs. These realities lead researchers across the globe to revisit the notion of 'privacy and data protection' to strike a balance between privacy invasion and enforcement. Malaysia is no exception. Nonetheless, there is no in-depth analysis of the adequacy of the current data protection regime in Malaysia. This article aims to fill that gap by revisiting the concepts of 'privacy' and 'data protection' and analysing the extensive literature in the field, keeping the Malaysian data protection regime in a special focus. The findings of this study reveal that in some respects, the data protection regime of Malaysia falls short of the global data protection standard. This study suggests that to strengthen the data protection regime of Malaysia, the policymakers may consider amending the *Personal Data Protection Act 2010* (PDPA) to make it in line with the international data protection standards and especially, the General Data Protection Regulation (GDPR).

Keywords: privacy, data protection, data protection regime in Malaysia, PDPA, GDPR.

I INTRODUCTION

In this era of information, Information Communication Technologies (ICTs) have enhanced the ability of governments, businesses and private individuals to operate

* PhD Candidate, Faculty of Law, University of Malaya; Assistant Professor, Department of Law and Justice, Bangladesh University of Business and Technology (BUBT).
** Retired Professor of Law, Faculty of Law, University of Malaya.
*** Senior Lecturer, Faculty of Law, University of Malaya.

surveillance, intercept communication and collect large scale personal data. These matters ultimately pose huge threats to the right to privacy and personal data of individuals.

Further, the data protection regime of a jurisdiction faces numerous challenges including (1) the gaps in scope; (2) addressing latest technologies; (3) governing trans-border data flows; (4) striking a balance in surveillance and data protection; (5) enhancing enforcement; (6) ascertaining jurisdiction and (7) handling the compliance issues.[1] Hence, in recent decades, privacy appears as one of the pressing issues in contemporary global political agenda.[2]

In such a context, the law has to reconcile the conflicting interests of individuals in an ever-complex society, while the judiciary has to determine whether the right to privacy is to be upheld.[3] There is no explicit provision regarding the right to privacy in the Federal Constitution of Malaysia, although some sort of privacy is recognised in the constitutions of nearly 130 countries of the world.[4] This stand of the Malaysian Constitution raises a substantial question as to whether privacy can be labelled as one of the fundamental rights in Malaysia. In *Ultra Dimension Sdn Bhd v Kook Wei Kuan*,[5] Justice Faiza Tamby Chik unequivocally asserted that Malaysian laws do not recognise the right to privacy.[6] In reaching this conclusion, the Malaysian High Court referred to another famous case,[7] in which it was held that the right to privacy is not acknowledged in the English common law. Justice Faiza Tamby Chik reasoned that since English common law is applicable in Malaysia pursuant to s 3 of the *Civil Law Act* 1956, privacy rights which are not recognised under English Law is accordingly not recognised under Malaysian law.

It may be relevant to state that there exist isolated privacy provisions in a wide array of domestic laws of Malaysia, as discussed briefly in part V of this article. These scattered privacy provisions which are embedded in numerous laws do not provide adequate protection for privacy and personal data in the digital age; thus, a comprehensive data protection law is needed.

Following from this, Malaysia has enacted the *Personal Data Protection Act 2010* (PDPA) to introduce a systematic data protection regime in the country. The PDPA sets the basic standard for data processing activities for individuals, businesses and other entities in Malaysia. It establishes an extensive cross-sectoral system of data protection regime regarding commercial transactions, the key enabler to enhance the trust of consumers

---

1 Technology and Logistics Division, UNCTAD, *Data Protection Regulations and International Data Flows: Implications for Trade and Development* (UNCTAD/WEB/DTL/STICT/2016/1/iPub, April 2016) xii.

2 Md Toriqul Islam, Abu Bakar Munir, Siti Hajar Mohd Yasin and Ershadul Karim, 'Data Protection Law in Asia' (2018) 8(4) *International Data Privacy Law* 338.

3 John J Thauberger, 'Right to Privacy' (1965) 30 *Saskatchewan Bar Review* 30, 167. See also Adekunle, Adedeji and Irekpitan Okukpon, 'The Right to Privacy and Law Enforcement: Lessons for the Nigerian Judiciary' (2017) 7 (3) *International Data Privacy Law* 202.

4 'What Is Privacy?', *Privacy International* (Web Page) <https://privacyinternational.org/explainer/56/what-privacy>.

5 [2001] MLJU 751.

6 Ibid 757.

7 *Kaye v Robertson* (1991) FSR 62.

in business and e-commerce by addressing an increased number of credit card frauds, identity thefts, and sale of personal data without the consent of the persons concerned.[8]

Above all, the PDPA is a unique data protection legislation in Malaysia. However, it has several shortcomings in comparison with the latest global data protection standard, especially the General Data Protection Regulation, 2018 (GDPR). Against this backdrop, this article attempts to offer a general overview of the right to privacy in Malaysia, covering the emergence, meaning, and its value, together with a holistic examination of the data protection regime in Malaysia. The article concludes with some suggestions that the Malaysian policymakers may consider in amending the PDPA to secure a safer online eco-system in Malaysia.

II UNDERSTANDING PRIVACY

The right to privacy has gone through a long process in its development. It has been said that the debate over privacy concerns is as old as human beings.[9] We may depict this long historical journey of privacy as the long walk to personal freedom. Earlier, legal norms approved only a few rights such as the right to life, right to property, and so forth. Subsequently, the law started recognising numerous other human interests such as feelings, sensitivity, emotions, and intellect.[10]

Gradually, the notion of the 'right to life' began to apply horizontally to cover a wide array of rights, including 'the right to be let alone',[11] popularly known as the 'right to privacy' as coined by Warren and Brandeis.[12] Due to long-standing support and recognition in the national, regional and international legal instruments, the desire for personal freedom reached such an extent that people were no longer interested to share their personal affairs with everyone, and would prefer to do so with selective persons. The authors prefer to treat this trend as the right to privacy in the digital age.

In today's data-driven world, there has been monetisation of data, and thus, personal data has appeared as a Holy Grail, turning it into a commodity, and accordingly, being sold and bought.[13] Diverse actors often pile up reams of personal data, through various means, for multiple purposes posing tremendous challenges to our personal life. Privacy is crucial for the wellbeing of a free society, thus no one can violate it unless there remains a pressing State interest.[14] Hence, the right to privacy is to be respected from the cradle to the grave.

Nevertheless, it is a huge challenge to protect privacy in this era of ubiquitous computing. Denis O'Brien, for example, lamented that maybe the right to privacy is a charming idea to the philosophers but not to the legislators, who try to place it within the

---

8 Shanthi Kandiah, 'Malaysia' in Alan Charles Raul (ed) *The Privacy, Data Protection and Cybersecurity Law Review* (Law Business Report Research, 6th ed, 2019) 251.

9 Jan Holvast, 'History of Privacy' in *The History of Information Security* (Elsevier, 2007) 737-69.

10 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) *Harvard Law Review* 193.

11 Thomas McIntyre Cooley, *A Treatise on the Law of Torts* (Callaghan, 1930) Vol 2.

12 Warren and Brandeis (n 10) 1.

13 JW Jerome, 'Buying and Selling Privacy Big Data's Different Burdens and Benefits' (2013) 66 *Stanford Law Review* 47.

14 Larry M Elison and Dennis NettikSimmons, 'Right of Privacy' (1987) 48(1) *Montana Law Review* 1.

legal framework.[15] To the legislators, privacy is a pressing problem in terms of explaining it with precision, determining its boundaries, and suggesting remedies in case of its invasion. This landscape widened the philosophy 'the right to be let alone' to capture more complexities encompassing privacy, and associated economic, social, political, psychological, and legal concerns. Hence, the conceptualisation of privacy has not lost its appeal, rather, it has led the researchers to revisit and rethink this right in the digital age. Thus, in the following section, a short account of privacy covering its history of emergence, meaning and value is covered.

A *Emergence of Privacy*

Even though privacy seems to be a newly emerged notion, it can be found in the ancient codes and texts of the Greeks, Romans, and the Anglo-Saxon ages.[16] There were also references to privacy in both ancient anthropological and sociological discourses.[17] It is believed that Aristotle attempted, for the first time in history, to distinguish private and public life,[18] and later, the Romans advanced with the idea and approached to protect privacy judicially.[19] Thus, Aristotle's demarcation on the public-private sphere of politics, i.e., the *polis* and *oikos*, two separate circumferences of life, was identified as the early references to privacy.[20] This public-private construction was also employed to mean the domain of national authority, in contrast, the self-regulation, as described in John Stuart Mill's essay, *On Liberty*.[21] A similar justification appears in Locke's 'Second Treatise on Government' as well.[22] Despite the series of the awareness of privacy in the long past, the emergence of privacy has become evident in the late 19th century, although most people have become conscious about privacy mostly in the past century.[23]

Indeed, the modern construction of the notion of 'privacy' surfaced first in 1890 through a seminal piece 'The Right to Privacy' by Louis Brandeis and Samuel Warren.[24] On 25 January 1883, Samuel Dennis Warren, a famous American author and attorney, got married to Miss Mabel Bayard, the daughter of Thomas Francis Bayard, a former US Senator. One day, they spent intimate moments at the exclusive Back Bay section in Boston. Later, the 'Saturday Evening Gazette' in its specialized 'Blue Blood Items'

---

15 O'Brien, 'The Right of Privacy' (1902) 2 *Columbia Law Review* 445.

16 Samuel H Hofstadter, Samuel Dennis Warren and Louis Dembitz Brandeis, *The Development of the Right of Privacy in New York* (Grosby Press, 1954); Roscoe Pound, 'Interests of Personality [Concluded]' (1915) 28 (5) *Harvard Law Review* 445.

17 Metaphysics Research Lab, Stanford University, *Stanford Encyclopaedia of Philosophy* (online on 22 March 2020) (Spring ed, 2018), 'Privacy'.

18 Rhys Smith and Jianhua Shao, 'Privacy and E-Commerce: A Consumer-centric Perspective' (2007) 2(7) *Electronic Commerce Research* 89.

19 Stanford Encyclopaedia of Philosophy (n 17).

20 Ibid.

21 John Stuart Mill, 'On Liberty', *A Selection of His Works* (Springer, 1966) 1-147.

22 John Locke, *Second Treatise of Government: An Essay Concerning the True Original, Extent and End of Civil Government* (John Wiley & Sons, 2014).

23 George Edward Richie, 'The Role of the Epistemic Community in Influencing Privacy Legislation: The United State and The European Union' (PhD Thesis, University of Denver, 2010).

24 Warren and Brandeis (n 10).

published their passionate intimate moments with shocking details.[25] This incident embarrassed Warren immensely, and subsequently, he discussed it with his friend Louis Brandeis, an American lawyer and Associate Justice of the US Supreme Court.[26] Consequently, their thoughts and written work on that issue created history.

Warren and Brandeis started inquiring into the existing legal principles whether there were any provisions for preventing that intrusion of Warren's privacy and became convinced that the conventional torts for libel and slander were not sufficient. They discovered that there was no law recognising the principles by way of which damages may be awarded for the violation of one's feelings.[27] They mourned for the personal life of individuals and warned people about its invasion. They wrote the words 'leave me alone', and henceforth, introduced, what judges referred to as 'the right to be let alone'.[28] From then onwards, the right to privacy has been recognised in almost all legal systems in the civilized world.

B *Meaning of Privacy*

The term 'privacy' is a notion that is full of fascinating and distinctive features but not clearly understood. Richard A. Posner, for example, remarked that privacy is an elusive and poorly defined conception.[29] Being abstract, privacy is not an easy-going concept. Thus, much ink has been spilt in attempts to define the term 'privacy'. Besides, privacy and technology shape and mould each other in the contemporary world. Hence, privacy protection mechanisms may not work unless it is designed while looking at technological developments.

Over the years, many scholars from different disciplines have attempted and continue to conceptualise privacy in a wide range of tones. In the present study, the researcher aims to explain the meaning of the notion of 'privacy' by analysing these scholarly works as offered by famous legal scholars.

Some scholars attempt to explain the notion of 'privacy' by demonstrating its synonyms. For example, to paraphrase Ruth Gavison, privacy has some constituent components, such as anonymity, solitude, and secrecy.[30] Helen Nissenbaum classifies privacy as a dynamic and complex issue, and the sensitivity to the data in terms of the purpose, context, and trust.[31] Westin attempted to articulate privacy in terms of social, personal, and regulatory dimensions.[32] While Anita Allen surmises that privacy

---

25 James H Barron, 'Warren and Brandeis, the Right to Privacy, 4 Harv. L. Rev. 193 (1890): Demystifying a Landmark Citation' (1979) 13 *Suffolk University Law Review* 875. See also Alpheus Thomas Mason, *Brandeis: A Free Man's Life* (Plunkett Lake Press, 2019).

26 Robert Sprague, Kevin Grauberger and Nicole Barberis, 'One Hundred Twenty Years of US Privacy Law Scholarship: A Latent Semantic Analysis' (2015) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2602904>.

27 Warren and Brandeis (n 10) 195.

28 PJ Gray-Lukkarila, 'The Right to Privacy: Constitutional and Theoretical Foundations' (PhD Thesis, The Claremont Graduate University, 1997).

29 Richard A Posner, 'The Right of Privacy' (1977) 12 *Georgia Law Review* 393.

30 Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89(3) *The Yale Law Journal* 421.

31 Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 1(79) *Washington Law Review* 119.

32 Alan F Westin, 'Social and Political Dimensions of Privacy' (2003) 59(2) *Journal of Social Issues* 1.

appears in the multifaceted denominations, such as physical, proprietary, decisional, and informational.[33]

William Parent volunteers to offer a viewpoint of privacy that is harmonious to the common expression and does not exaggerate or disconcert the central idea of other key terms. To him, privacy denotes the state of not getting their personal data stored, noticed or owned by others.[34] This is no doubt an estimable definition, but there remain questions as to its conciseness. Furthermore, the definition contains a descriptive account and is devoid of any normative principle.

Observing the intricacies encompassing the meaning of privacy, Daniel Solove argues that the notion of 'privacy' is full of disarray; hence, none can enunciate its proper meaning. Moreover, privacy encompasses numerous aspects and includes many things, such as freedom of thought against surveillance, control over one's own body, and personal data, aloneness in residence, the capacity of protecting reputation, and safeguard against searches and questionings.[35] While articulating privacy as a tort, D. W. Prosser emphasised that privacy does not contain one, but rather a group of *four* torts, such as-

> (1) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; (2) public disclosure of embarrassing private facts about the plaintiff; (3) publicity which places the plaintiff in a false light in the public eye; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[36]

Adam Moore is of the view that privacy refers to the right to have control in the access to premises, places, and personal data, and together with the usage and controlling powers thereof.[37] He argued that there is hardly any definition of privacy that can please everybody. Besides, the evaluation and justification of privacy in society play a crucial role in rendering dimensions to the definition, and hence, any endeavour of defining privacy would perhaps always be incomplete.[38]

Indeed, the notion encompassing privacy is not generally unified, but rather it varies in diverse features, scope, and nature based on locality, society, culture, custom, moral values, etc. Though there are differences among the scholars about privacy in terms of concepts and contexts, certain things are common as to the notion as shared by all discourses. For example, all privacy-related discourses acknowledge that privacy is an intrinsic human right; it facilitates the individuals to exile the outsiders from their intimate zone, and it uplifts the dignity and other constitutional guarantees of humankind. The Australian Privacy Charter, for example, states, 'privacy is such a value, which underpins human dignity and other key values, e.g., freedom of association and freedom of speech'.[39]

---

33 Anita L Allen, 'Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm' (1999) 32 *Connecticut Law Review* 861.

34 WA Parent, 'Privacy, Morality and the Law' (1983) 12(4) *Philosophy and Public Affairs* 269.

35 Daniel J Solove, *Understanding Privacy* (Harvard University Press, 2008) vol 173.

36 William Lloyd Prosser, 'Privacy' (1960) 48 *California Law Review* 383.

37 Adam Moore, 'Defining Privacy' (2008) 39(3) *Journal of Social Philosophy* 410.

38 Ibid.

39 Council, Australian Privacy Charter, 'Australian Privacy Charter' (1994) *Australian Privacy Charter Council* <http://www.privacy.org.au/apcc/charter.html>.

From the above discussion, it is apparent that the term 'privacy' incorporates a wide range of issues within its domain. Therefore, to offer a precise definition of privacy is almost impossible. Nonetheless, privacy is explained as a matter of protecting one's private spheres from the interference of others, though due to the complexities in this information era, the distinction between private and public domain is not easy to draw. However, we may prefer to share Blaine Thacker's definition as an acceptable definition of privacy. To paraphrase Thacker, privacy refers to the *claim of the persons, groups, or organisations to determine how, when, and to what extent their information will be shared with others*.[40]

C *Value of Privacy*

The evolving information age is transforming our lives in ways that we could never have imagined. Nowadays, privacy is a pressing concern due to numerous reasons, such as - the globalization of human communication, the commercial importance of data, the interest of governments in accessing and processing data, voluntary data sharing by people on social media, the commercialization of personal data and the usage of cloud computing – coupled against the recognition of privacy as one of the fundamental human rights, such as freedom of speech.[41]

Since long ago, governments across the world have conducted diverse surveillance programs for safety, security, public order, or on public interest grounds. George Orwell once warned in his dystopian novel entitled '*1984*' that Big Brother (a fictional character to refer to the government authorities) is always watching you.[42] Focusing on the governmental interests on people's activities, George Orwell wrote:

> It was even conceivable that they watched everybody all the time. But at any rate, they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.[43]

Rotenberg remarked back in 1996 that '[p]rivacy will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial society of the 20th century'.[44] His prediction has become reality as privacy emerges as one of the most desired interests in current times. Besides, in this data-driven society, people deliberately share large amounts of personal data on social media, and to

---

40 Justice, Canada. Parliament. House of Commons. Standing Committee on, Solicitor General and Blaine A Thacker, *Open and Shut: Enhancing the Right to Know and the Right to Privacy: Report of the Standing Committee on Justice and Solicitor General on the Review of the Access to Information Act and the Privacy Act* (Queen's Printer for Canada, 1987).

41 Christopher Kuner et al, 'The Extraterritoriality of Data Privacy Laws—An Explosive Issue Yet to Detonate' (2013) 3 (3) *International Data Privacy Law* 147.

42 George Orwell, *Nineteen Eighty-Four* (Everyman's Library, 2009).

43 Ibid Part One, Section 1.

44 James Gleick, 'Big Brother Is Us', *The New York Times* (online 29 September 1996) <http://www.nytimes.com/1996/09/29/magazine/big-brother-is-us.html?pagewanted=all&src=pm>.

numerous public and private bodies. Nevertheless, there must be a balance between the compelling necessities of data sharing and the right to privacy of individuals.

Interestingly, privacy is essential not only for human beings but also for animals. Fascinated by the outputs of various animal and cultural studies, Alan Westin, for example, remarked that the basic outcomes of animal studies reveal that every animal essentially searches for its privacy in the small-group intimacy.[45] Westin added that the ecological studies have shown that the scarcity of intimate space due to congestion may cause huge threats to survival.[46] Some other authors argue that due to the lack of intimate private space, beasts may destroy themselves, or grossly involve in the suicidal decreasing of their population.[47] For example, while experimenting with mice and sloths in cages, Calhoun, noticed that a certain proportion of space is inevitable for each species and the lack of which leads to the splitting in friendly relations and causes diverse illnesses, such as heart failure and an increase of blood pressure.[48]

In line with the above philosophy, it can be argued that the right to privacy is essential for the well-being and prosperous life of almost all animals in the world. Besides, in the absence of privacy protection mechanisms, people might incur numerous irreparable losses. For instance, data revelation may cause one to wreck his marriage, or the news of addiction to alcohol or illicit drugs may be sufficient for losing one's job.

Some scholars even identify that privacy is important for democracy, though the relationship between them is a complex and dynamic one and there are diverse disagreements between them.[49] Privacy may be compromised in a democracy by the polling agents, who endeavour to mobilise, involve and stimulate voters to vote– or not to vote. Today, we see the massive roles of polling agents, particularly in social media, to manipulate the voter's psychology. All these eventually influences the result of the election and creates debates in the political discourses.

This strategy was applied by the election campaign of Barack Obama both in the 2008 and 2012 US general elections. The summary of these techniques includes an unprecedented ability to use advanced technologies to influence targeted voters and precisely specified constituencies with a tailored message in both online and offline formats.[50] There were allegations against former US President Donald Trump that his election campaigns used the voter suppression strategy in the 2016 US election by sending negative messages (dark posts), based on race, ethnicity, and socio-economic status by using the advertising tools of Facebook.[51] Therefore, the issue is no longer restricted to the

---

45 Alan F Westin, *Privacy and Freedom* (Atheneum, 1967) vol 7.

46 Ibid.

47 Adam D Moore, 'Privacy: Its Meaning and Value' (2003) 40(3) *American Philosophical Quarterly* 215.

48 John B Calhoun, 'The Study of Wild Animals Under Controlled Conditions' (1950) 51 *Annals of the New York Academy of Sciences* 1113.

49 Colin Bennett and Smith Oduro Marfo, *Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities*, International Conference of Data Protection and Privacy Commissioners (ICDPPC) 7.

50 Colin Bennett, 'The Politics of Privacy and the Privacy of Politics: Parties, Elections and Voter Surveillance in Western Democracies' (2013) *First Monday* 1.

51 Bennett and Smith (n 49) 3.

privacy of the individual voter, but rather, correlates to greater issues such as democracy and politics of the day.

Above all, privacy matters because we all wish to have a personal life and like to share our correspondence and memories with only those whom we trust. Whereas in a pure democratic culture, personal liberty includes the autonomy and freedom of individuals from the unauthorised access of the businesses, or diverse public and private actors. Indeed, in a networked society, privacy is more valued than any other rights, because, in current times, we cannot help but share our valuable and personal information to numerous bodies as a course of modern lifestyle, despite knowing the vulnerability of our rights. Therefore, it would be disastrous, if any of these actors leak, in any way, our sensitive personal data. Undoubtedly, these losses will be unthinkable, as most of them are irreparable, and hardly they admit any substitutes or compensation.

III THE EMERGENCE OF DATA PROTECTION

The phrase 'data protection' usually, covers two specific things, namely (1) the standard to deal with one's personal data and (2) the followed practices to secure and uphold that standard.[52] Indeed, data protection or data privacy is more than a relationship among a wide array of issues, such as data collection, sharing or transfer, and legal, political, technological, and public demand encompassing them.[53] Sometimes, it is described as a notion which rises from an attempt to strike the balance among some contesting groups, and sometimes, it can be presented as an output of certain chain reactions.[54] To put it simply, data protection refers to the law adopted for the protection of personal data which is likely to be processed, collected, and retained through automation or any other profiling means. Data protection law monitors how governments, businesses, or other organisations use the personal data of individuals.[55] Therefore, data protection means such a mechanism that enables individuals to take lawful control over their personal data.

Whilst talking about data protection, it is equally essential to focus on personal data and sensitive personal data, as by data protection, we usually mean the protection of these two. Personal data means any information about an identifiable natural person (data subject) who may be recognised directly or indirectly, by using some identification signs, such as the person's name, identification (ID) number (including online ID), socio-economic and cultural identity, location data, or data relating to any specific physical, physiological, genetic or mental condition.[56] Under the Malaysian PDPA, personal data implies any information regarding commercial transactions, which is-

---

52 Angus Hamilton and Rosemary Jay, *Data protection: Law and Practice* (Sweet & Maxwell, 2003) 1.

53 MG Michael, *Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies: Emerging Technologies* (IGI Global, 2013).

54 Hamilton and Rosemary (n 52).

55 'Data Protection' *GOV.UK* (Web Page) <https://www.gov.uk/data-protection>.

56 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) [2016] OJ L 119/1, art 3(2).

> (a) being processed entirely or partially employing equipment operating automatically in response to instructions given for that purpose; (b) recorded with the intention that it should wholly or partly be processed employing such equipment; or (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, and relates directly or indirectly to a data subject, identified or identifiable from that or other information possessed by the data user, including any sensitive data or expression of opinion regarding the data subject, but shall not include any information processed to carry on a credit reporting business by a credit reporting company under the Credit Reporting Agencies Act, 2010.[57]

Therefore, to assume 'personal data' under the purview of the PDPA, a piece of information must meet at least three conditions. *Firstly*, the data must be in respect of a commercial transaction; *secondly*, it must be processed either electronically or manually as part of a filing system, and *lastly*, it must connect directly or indirectly to a data subject, identified or identifiable from that information or other information held by the data user.[58] Simply speaking, **personal data** refers to such pieces of data which, by a combined reading, leads to the identification of an identifiable natural person. In the context of Malaysia, the *MyKid*,[59] *MyKad*,[60] driving license and passport are certain official documents that contain the personal data of the Malaysian nationals.[61]

Sensitive personal data means a wide range of information, such as the person's physical or mental health, religious, political or other beliefs or views, criminal records, and together with such other personal information about data subject as determined and published in the Official Gazette by the concerned Ministry.[62]

However, from time immemorial, data in respect of persons are collected, retained, exchanged in diverse ways or transferred to the third parties for multiple purposes. Thus, data collection is one of the old habits, though it may not be the old profession.[63] The threats on data privacy arise from numerous public-private entities encompassing chiefly the health sector, criminal justice system, financial sector, location data, academic research, and online activities. The threats upon personal information are often identified as identity theft or fraud, misprocessing, mishandling or misapplication of personal data.[64]

Whatever the case may be, in the networked world, protecting personal data has become increasingly challenging because of several factors, such as emerging technologies, modern business models, services and systems, growing reliance on different

---

57 *Personal Data Protection Act 2010* (Act 709) (Malaysia) (PDPA) s 4.

58 Shanthi Kandiah (n 8) 253.

59 The *MyKid* is the identity card for Malaysian children under 12 years old which contains specific personal data, including information regarding birth date, health and education. See Noriswadi Ismail, *Understanding Personal Data Protection Law* (LexisNexis, 2013) 1.

60 Malaysian citizens above 12 years old are bound to register compulsorily for this national registration identification card and they hold this card till death. See Ismail (n 59).

61 Ibid 2.

62 PDPA (n 57) s 4.

63 Ibid.

64 Andrew Murray, *Information Technology Law: The Law and Society* (Oxford University Press, 2nd ed, 2013).

analytics, Big Data, tracking of data, sharing or profiling, and artificial intelligence.[65] Further, the atmospheres and surroundings in which we live, gets through, generates and assembles much more information on human conduct. Furthermore, the appliances we use or set up into our residences such as communication devices, transportation and street systems, all produce reams of data. This backdrop requires the emergence of data protection regulations to strike the balance among the interests of the governments, business entities, and private individuals.

Consequently, regional and international regulatory frameworks have been introduced to secure data protection around the globe. Among these, the notable instruments are, *inter alia*, the OECD Privacy Guidelines (1980), the OECD Privacy Framework (2013), the Convention 108 of Council of Europe (1981), the Modernised Convention 108 of Council of Europe (2018), the UN Guidelines for the Regulation of Computerized Personal Data Files (1990), the UN Principles on Personal Data Protection Privacy (2018), the Reports of the Special Rapporteur on the Right to Privacy in the Digital Age 2016-2020, the APEC Privacy Framework 2005, the APEC Privacy Framework (2015), the ASEAN Framework on Personal Data Protection (2016), the EU Directive 95/46/EC, and the General Data Protection Regulation, 2018 (GDPR). Besides these, privacy has been recognised by many other international and regional human rights instruments.[66]

At the national level, there has been a wave of data protection law enactments, especially, in the last two decades. It started from the *Hessian Data Protection Act* (*Hessisches Datenschutzgesetz*), 1970 of Germany, followed by Sweden, France, Germany, Denmark, Austria, Norway, and the USA. To date, a total of 143 countries have enacted data protection laws,[67] and many other nations are attempting to do the same. In Malaysia, the Personal Data Protection Act (PDPA)[68] (Act No. 709) was passed on June 2, 2010 and came into effect on 15 November 2013.[69]

---

65 'Data Protection', *Privacy International* (Web Page) <https://privacyinternational.org/topics/data-protection>.

66 The human rights instruments that contain privacy provisions include, among others, the Universal Declaration of Human Rights, 1948 (art 12); International Covenant on Civil and Political Rights, 1966 (art 17); the United Nations Convention on Migrant Workers, 1990 (art 14); the United Nations Convention on the Rights of the Child, 1989 (art 16); African Charter on the Rights and Welfare of the Child, 1990 (art 10); the Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019 (art 4); American Convention on Human Rights, 1969 (art 11); American Declaration of the Rights and Duties of Man, 1948 (art 5); Arab Charter on Human Rights, 1994 (updated in 2004) (arts 16 and 21); ASEAN Human Rights Declaration, 2012 (art 21), and European Convention on Human Rights, 1950 (art 8).

67 A 2020 article of Greenleaf and Cottier reveals that so far, a total of 142 countries have enacted the data protection laws across the globe. At the time of writing, it is estimated that there are at least 143 countries with data protection laws. See generally, Graham Greenleaf and Bertil Cottier, '2020 Ends a Decade of 62 New Data Privacy Laws' (2020) 163 *Privacy Laws & Business International Report,* 24-6.

68 Edwin Lee Yong, 'Personal Data Protection and Privacy Law in Malaysia', *Beyond Data Protection* (Springer, 2013) 5-29.

69 Abu Bakar Munir, Siti Hajar Mohd Yasin and Md Ershadul Karim, *Data Protection Law in Asia* (Sweet & Maxwell/Thomson Reuters, 2018) 209.

IV DATA PROTECTION REGIME IN MALAYSIA

In the last few decades, the issue of privacy and personal data protection has gained increased attention in many parts of the world, including Malaysia. In the current section of this article, the gradual development of privacy and data protection issues in diverse legal contexts of Malaysia is analysed. Additionally, this section will also summarise the shortcomings of the Malaysian data protection regime and conclude with certain workable suggestions for strengthening the same. While doing so, it is equally important to focus on the contextual surroundings of the data protection regime in Malaysia. By contextual surroundings, the treaty obligations regarding privacy and the recognition of privacy in the Malaysian Federal Constitution, and other existing laws will be discussed.

With respect to treaty obligations, the provisions of the Universal Declaration of Human Rights (UDHR) 1948 and the International Covenant on Civil and Political Rights (ICCPR) 1966 are worthy of discussion here. It may be relevant to state that the 'right to privacy' became an international human right before it was constitutionally recognised as a fundamental right.[70] The right to privacy was recognised first in the UDHR when States' Constitutions ensured only a few aspects of privacy, for example, the inviolability of one's home and correspondence. For instance, Article 12 of the UDHR provides,

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

17 years later, privacy was recognised in Article 17 of the ICCPR using similar language as in Article 12 of the UDHR. The only difference between the two documents implies that Article 17 of the ICCPR not only prevents the 'arbitrary' interventions in one's privacy and associated rights but also the 'unlawful' ones.

Since the UDHR is not a treaty or a convention, its provisions are not obligatory for the Member States of the United Nations but remains as an international obligation for the signatories of the ICCPR. As Malaysia has not signed the ICCPR, it does not have any international treaty obligations concerning privacy.[71]

Being an ASEAN Member State, Malaysia is a signatory to the ASEAN Human Rights Declaration, 2012. Malaysia is also part of the Asia Pacific Economic Cooperation (APEC), and accordingly, is assumed to be attached with the APEC Privacy Framework, 2015. However, Malaysia is not a signatory to the APEC Cross-border Privacy Rules (CBPR), 2005 (updated in 2015). Consequently, it appears that Malaysia does not have any binding international or regional commitment toward the recognition or protection of

---

[70] O Diggelmann and MN Cleis, 'How the Right to Privacy Became a Human Right' (2014) 14 *Human Rights Law Review* 441.

[71] Other than Malaysia, the countries that have not yet ratified the ICCPR include- Qatar, Singapore, Sao Tome & Principe and St. Lucia. Among all, Malaysia, Qatar, Singapore have never signed the ICCPR, whereas Sao Tome & Principe and St. Lucia have signed but not ratified the ICCPR. See generally, Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (Oxford University Press, 2014) 321.

the right to privacy. It is worth mentioning that there are only five UN Member States with data protection laws, but have never ratified the ICCPR, and Malaysia is one of them.[72]

Regarding the recognition of privacy in the national constitution, it is to be noted that the Federal Constitution of Malaysia does not recognise the right to privacy in the 'fundamental liberties', or any other parts thereof. The Malaysian courts have dismissed the claims of privacy as an invasion of common-law tort. For example, in the *Ultra Dimension Sdn Bhd v Kook Wei Kuan* case,[73] the Malaysian High Court rejected a petition that claimed damages on the ground of violation of privacy and breach of confidence. In *this case*, Justice Faiza Tamby Chik, in declaring that Malaysian laws do not recognize the right to privacy, said as follows:[74]

> I am of the view that it is clear that English law does not recognise privacy rights and it, therefore, follows that invasion of privacy rights does not give rise to cause of action. As English law is applicable in Malaysia pursuant to section 3 of the Civil Law Act 1956, privacy rights which [are] not recognised under English law [are] accordingly not recognised under Malaysian law.

Similarly, in *Dr Bernadine Malini Martin v MPH Magazine Sdn Bhd & 2 Lagi*,[75] the Court of Appeal observed that 'the law of this country, as it stands presently, does not consider the invasion of privacy as an actionable wrong'.

However, some scholars have pointed out that in several cases, the Malaysian judiciary have argued that the Federal Constitution of Malaysia recognises the right to privacy.[76] For example, in *Re Kah Wai Video Bhd*,[77] it was held that the operation of search and seizure infringes the right to property under Article 13 of the Federal Constitution.[78] The viewpoint was based on the decision of an Indian case, *Sharma & Ors v Satish Chandra,*[79] in which the same issue was raised under Article 19 of the Indian Constitution.[80] The Supreme Court of India held that such search and seizure were constitutional as conducted for a short period required for merely an investigation. In the same case, the court also acknowledged that privacy is a fundamental right.

Furthermore, in *Sivarasa Rasiah v Badan Peguam Malaysia & Anor case,*[81] the Federal Court observed, in the form of *obiter dicta*, that personal liberty as recognised in Article 5(1) of the Federal Constitution includes many rights, *inter alia*, the right to

---

72 Graham Greenleaf, Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey (2017) 145 *Privacy Laws & Business International Report*, 10-13; *UNSW Law Research Paper,* No. 17, 45.

73 [2001] MLJU 751.

74 Ibid 757.

75 (2010) 5 MLJ 755.

76 Abu Bakar Munir and Siti Hajar Mohd Yasin, Personal Data Protection in Malaysia: Law and Practice (Sweet & Maxwell Asia, 2010) 12-15.

77 (1987) 2 MLJ 459.

78 Munir and Yasin (n 76) 13.

79 AIR 1954 SC 300.

80 Munir and Yasin (n 76) 13.

81 (2010) 2 AMR 301; (2010) 2 MLJ 333.

privacy.[82] Taking note of this, it has been remarked that it is likely that some protection of privacy could still develop through the Federal Constitution of Malaysia.[83]

Article 5(1) of the Federal Constitution states that 'no person shall be deprived of his life or personal liberty save in accordance with law'. The right to life and personal liberty shall have to be interpreted widely to cover all physical and emotional aspects of humankind, and that essentially includes the privacy of persons and human dignity. Warren and Brandeis, for example, asserted that some human affairs, e.g., pleasure and enjoyment may not be noticed in the material objects but in the human feelings, emotions and thoughts that form an indispensable portion of human personality.[84] Moreover, privacy is also essential to lead a quality life, as it is argued that privacy protects the interests of individuals in becoming, being, and remaining as a person.[85]

Hence, the *Sivarasa* case may be considered to set the basis for the protection of a constitutional right to privacy in Malaysia. Though in principle, the lower courts are duty-bound to obey the precedent of the Federal Court, strangely, several lower courts have endorsed this right in subsequent cases but with no reference to the judgement of *Sivarasa case*.[86] Besides, in several cases, the Malaysian High Court also recognised privacy on different grounds, such as the preservation of modesty, decency and human dignity,[87] or the autonomy, dignity, self-esteem and comfort of the plaintiff.[88] Given these matters, it is hoped that the Federal Court may have an opportunity to make a clearer statement on the fact once and for all.

Despite the above-mentioned stand of the Federal Constitution, the term 'privacy' appears in a number of statutes and regulations of Malaysia, such as Births and Death Registration Act 1957 (s. 4(4) (b)), Private Hospitals Regulations 1973, Penal Code 1976 (s. 509), Law Reform (Marriage and Divorce) Act 1976 (s. 46A (2) (b)), Private Healthcare Facilities and Services Act 1998 (s. 107 (2) (ii)), Communication and Multimedia (Licensing) Regulations 1999, Child Act 2001 (s. 12(2)) and Credit Reporting Agencies Act (CRRA) 2010 (s. 30(5) (c)).

Among the above laws, the provisions of the Penal Code 1976 are especially worth mentioning, as s. 509 of the enactment explicitly recognised privacy under the heading of 'word or gesture intended to insult the modesty of a person'. Section 509 of the Act states,

> Whoever intending to insult the modesty of any person utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen by such person, or intrudes upon the privacy of such person, shall be punished with imprisonment for a term which may extend to five years or with fine or with both.

---

82 Munir and Yasin (n 76) 15.

83 Greenleaf, *Asian Data Privacy Laws* (n 71) 321.

84 Warren and Brandeis (n 10) 194.

85 Jeffrey H Reiman, 'Privacy, Intimacy, and Personhood' (1976) *Philosophy & Public Affairs* 44.

86 Munir, Yasin and Karim (n 69) 214.

87 *Lee Ewe Poh v Dr Lim Teik Man & Anor* 25 [2011] 1 MLJ 835 (HC), 8.

88 *Lew Cher Phow @ Lew Cha Paw & Ors v Pua Yong Yong & Anor* [2011] MLJU 1195 (HC).

In addition, there are at least six other laws, in which there are references for privacy, although they are not directly connected to the issue of data protection.[89] These laws include (1) Banking and Financial Institutions Act (BAFIA) 1989 (Act 372), containing legal protection to the confidentiality of consumer data (Part XIII: Information and Secrecy) (subsequently repealed by the Financial Services Act, 2013 (Act 758)), (2) Communications and Multimedia Act (CMA) 1998 (with amendment—Act A1220/ 2004), providing that consumers can address affairs regarding concerns affecting the quality of services, which conceivably involve the data privacy (Part VIII; s. 189 (consumer forum), and s.190(2)(e) (matters for consumer code)), (3) Electronic Commerce Act (ECA) 2006 (Act 658), rendering additional protection to anybody wishes to manage and join in e-commerce transactions, including online and offline privacy issues (s. 4), (4) Digital Signature Act (DSA) 1997 (Act 562), which impose obligations of secrecy over the use of the digital signature (s. 72), (5) Official Secrets Act (OSA) 1971 (Act 88), which governs the use of confidential public records (s. 2B and 2C), and (6) the Electronic Government Activities Act (EGAA) 2007 (Act 680), which governs the recognition of e-messages and the fulfilment of its legal postulates in regulating e-government procurement effectively, but does not cover data protection of the parties contracting with the government.[90]

From the above, it is evident that Malaysian law ensures the protection of privacy in certain specific circumstances. The highest court has, in the form of *obiter dicta*, stated that the right to privacy is implicit in the right to life as embedded in Article 5(1) of the Federal Constitution. Although privacy is impliedly recognised under the cover of the constitutional right to life, this application is not horizontal but rather, vertical covering the State and citizens' relation. Nonetheless, the Malaysian courts have, in some exceptional instances, upheld the invasion of privacy as an actionable tort for the protection of modesty, decency and dignity of the plaintiff, reflecting the significance of moral values in Malaysian society.[91]

As stated earlier, Malaysia entered the elite club of countries with comprehensive data protection laws in 2010, through the enactment of the PDPA. However, in terms of the latest development in data protection frameworks, there remains a question as to whether the PDPA is adequate to ensure the protection of personal data of Malaysian citizens. In the following section, we would search for the answer to this question by examining some key aspects of the PDPA along with some of its the major shortcomings.

A *The Personal Data Protection Act 2010 (PDPA)*

After a wait of more than 10 years since the late 1990s, Malaysia enacted the PDPA in 2010. It was the first data protection legislation among the ASEAN nations.[92] The Act produced a significant impact on the data protection regimes in Malaysia and in the

[89] Noriswadi Ismail, 'Selected Issues regarding the Malaysian Personal Data Protection Act (PDPA) 2010' (2012) 2 (2) *International Data Privacy Law* 105.

[90] Ibid 105, 106.

[91] *Maslinda bt Ishak v Mohd Tahir bin Osman* [2009] 6 MLJ 826; *Lee Ewe Poh v Dr. Lim Teik Man*, [2011] 1 MLJ 835 (HC); *M. Mohandas Gandhi v Ambank (M) Berhad* [2014] 1 LNS 1025; *John Dadit v Bong Meng Chiat* [2015] MLJU 1961 and *Toh See Wei v Teddric Jon Mohr* [2017] MLJU 704.

[92] Munir, Yasin and Karim (n 69) 209.

region. It is noteworthy that the Malaysian Government drafted the PDPA in 1998 but did not take any action until November 2009. After progressing with several stages of redrafting, the PDPA was placed for the first reading in November 2009, and in May 2010, the Federal Parliament passed the PDPA. After receiving the Royal Assent, the Act was officially published in June 2010.[93]

After another three years, the PDPA came into effect on 15 November 2013. On this very day, the Malaysian Government issued and gave effect to some other subordinate legislation regarding data protection, such as Personal Data Protection Regulations, Personal Data Protection (Registration of Data User) Regulations, Personal Data Protection (Fees) Regulations, Personal Data Protection (Class of Data Users) Order, and Appointment of the Personal Data Protection Commissioner.[94]

The Malaysian journey to enacting data protection regime is a noble endeavour and paved the way for other ASEAN and Asian nations. Following the tracks of Malaysia, the Philippines enacted the Data Privacy Act on 8 September 2012, Singapore passed its Personal Data Protection Act on 15 October 2012, Indonesia passed the Electronic Information and Transactions on 25 November 2016 (amending its previous Law No. 11 of 2008) and Thailand enacted the Personal Data Protection Act (PDPA) on 28 May 2019.[95]

The PDPA applies to the processing of personal data conducted by entities operating in Malaysia but does not apply to the processing performed outside the border unless that is further processed in Malaysia.[96] The enactment is divided into 11 Parts and consists of a total of 146 sections. Some major provisions of the PDPA, include, amongst others, the application (s. 2); definition and interpretation (s. 4), personal data protection principles (s. 5), registration (ss. 13-20), rights of the data subjects (ss. 30-44), exemptions (ss. 44-46), provisions about commissioners (ss. 47-60), data protection fund (ss. 61-69), advisory committee (70-82), appeal tribunal (ss. 83-100), inspection, complaint and investigation (ss. 101-109), enforcement (ss. 110-127), miscellaneous (ss. 128-144), and savings and transitional provisions (ss. 145-146).

It is pertinent to mention that a detailed and comprehensive analysis for all provisions of the PDPA is neither intended nor required for this article. Therefore, for the purpose of this article, some key provisions of the enactment shall be analysed, such as application and scope of the Act, definition and interpretation of certain matters, data protection principles, registration of data users, rights of the data subjects, the function of the national data protection authority, transborder data transfer and enforcement mechanisms under the Act.

1 *Application and Scope*

The provisions regarding the application and scope of the PDPA are mostly conventional in nature, like all other data privacy laws around the world. The PDPA applies to any person processing personal data of individuals (the processor), and the person having control over processing activities.[97] The other provisions, for example, the establishment

93 Ismail 'Selected Issues regarding the Malaysian Personal Data Protection Act' (n 89) 106.
94 Munir, Yasin and Karim (n 69) 209.
95 DLA Piper, *Data Protection Laws of the World: Full Handbook* (2017).
96 PDPA (n 57) s. 3(2).
97 Ibid s. 2(1).

and equipment principles,[98] the exclusion of artistic, literary and journalistic works (except the Security Principle),[99] personal, family and household affairs,[100] and educational institutions, churches, and non-profit organisational activities are also typical in nature. However, problems lie in two sectors, where the PDPA only applies to commercial transactions, and the public sectors remain outside of its ambit.

There are several criticisms that can be brought against the PDPA. In particular, the PDPA falls short of several specific issues, such as the scope limitations, lack of independence of the Commissioner, loopholes in privacy principles, extra-territoriality issues and due diligence.[101] Above all, one of the weakest features of the PDPA is that it does not apply to the public sector at all.[102] Many other authors also identified that the non-application of PDPA over public authorities is one of the main shortcomings of PDPA.[103]

2 *Definition and Interpretation*

Section 4 of the PDPA provides the interpretations for a wide array of important terminologies, including personal data, sensitive personal data, data processor, processing, data user, the data subject and commercial transactions. The meaning of both the personal data and sensitive personal data have been discussed in Part III of the article, and the rest other terms are discussed below.

> **Data processor**
> Data processor, in respect of personal data, refers to a person other than an employee of the data user, who processes the personal data on behalf of the data user only, not for any of his purposes.[104]

> **Processing**
> In respect of personal data, processing means the collection, storing, holding, recording or conducting any operation on the personal data. It also includes some other issues encompassing personal data, such as adaptation, organization, alteration, retrieval, consultation, use, disclosure (through transmission, transfer, dissemination or otherwise), alignment, combination, correction, erasure or destruction.[105]

---

98 Ibid.
99 Ibid s. 45(2)(f).
100 Ibid s. 45(1).
101 Graham Greenleaf, 'Limitations of Malaysia's Data Protection Bill' (2010) *Privacy Laws & Business International Newsletter*, Vol 104, No 1, 1-4.
102 Ibid 1.
103 Ismail 'Selected Issues regarding the Malaysian Personal Data Protection Act' (n 89) 108.
104 PDPA (n 57) s. 4.
105 Ibid.

Data user
Data user means a person, who processes the personal data either alone or jointly with other persons, or who authorises, or has control over the processing of personal data, but shall not include a data processor.[106]

Data subject
Data subject refers to a person, who is the subject of the personal data.[107]

Commercial transactions
Commercial transactions imply any transaction of a commercial nature, being contractual or not, and includes affairs concerning the supply or exchange of goods or services, agency, investments, financing, and banking and insurance, but does not include a credit reporting business carried on by a credit reporting company under the Credit Reporting Agencies Act 2010.[108]

3 *Data Protection Principles*

At the heart of the PDPA, there are seven personal data protection principles as outlined in ss. 6 to 12. The principles include (a) General Principle (s. 6), (b) Notice and Choice Principle (s. 7), (c) Disclosure Principle (s. 8), (d) Security Principle (s. 9), (e) Retention Principle (s.10), (f) Data Integrity Principle (s. 11), and (g) Access Principle (s. 12). The PDPA obliges a data user to comply with these principles while processing personal data and a non-compliance, subject to ss. 45 and 46, shall lead to a fine not more than RM300,000 or imprisonment not exceeding for a term of two years or both.[109]

The potential weakness of the principles lies in the limitations on use and disclosure. For example, businesses can potentially misuse the limits of sharing the data to third parties simply by exposing the class of third parties to whom the data is likely to transfer.[110] Furthermore, the 'Security Principle' is comparatively weak, which requires the data users to take *practical* steps, instead of taking *reasonable* steps as often practised in other jurisdictions.[111]

4 *Registration of Data Users*

The Malaysian data protection legislation is undoubtedly a valiant effort that adds a unique and new taste to the increasing number of data protection legislation in the Asian region.[112] The PDPA prescribes the mandatory registration requirement for certain data users, which is a unique practice in the world.

---

106 Ibid.
107 Ibid.
108 Ibid.
109 Ibid s. 5(2).
110 Greenleaf, 'Limitations of Malaysia's Data Protection Bill' (n 101) 2.
111 Ibid 3.
112 Ibid 1.

For example, although the GDPR does not require such registration for the data users, Malaysia and a few other countries have had this provision.[113] The PDPA requires the mandatory registration for processing personal data of certain specific sectors, such as the communications, banking and the financial institutions, insurance, health, tourism and hospitalities, transportation, education, direct selling, services, real estate, utilities, pawnbrokers and moneylender.[114]

5 *Rights of the Data Subjects*

The PDPA grants many rights for individuals concerning the processing of their data, including the right of access to personal data (s. 30), the right to correct personal data (s. 34), the right to withdraw consent (s. 38), right to prevent processing likely to cause damage or distress (s. 42) and the right to prevent processing for purposes of direct marketing (s. 43).

It is worth mentioning that many of these rights are similar to the EU standard as evidenced by the latest GDPR. For example, Article 15 of the GDPR deals with the right of access to personal data. Article 16 includes provisions as to the right to rectify personal data. Article 7(3) deals with the data subject's right to withdraw consent and Article 18 contains provisions regarding the right to restriction of processing., Article 21(2) and (3) comprise provisions against direct marketing. Nonetheless, unlike the GDPR, the PDPA falls short of certain rights, including the right to be forgotten (Article 17 and recital 65 and 66), the right to data portability (Article 20), and the right not to be subject to automated decision making and profiling (Article 22).

6 *National Data Protection Authority*

To ensure an effective data protection regime, an independent supervisory body is a must. However, the PDPA does not make provision for this mainly because of the lack of independence of the Personal Data Protection Commissioner. This can be inferred from the fact that the Personal Data Protection Commissioner's appointment,[115] allowance, remuneration,[116] and dismissal[117] are determined by the Minister, who, in turn, makes the Commissioner less independent.[118] Additionally, the Commissioner is responsible to produce an annual report to the concerned Minister. This annual report does not need to be tabled before Parliament.[119] Moreover, the PDPA also explicitly asserts that the Commissioner is responsible to the Minister and shall perform his or her responsibilities

---

113 These countries include Argentina, Bahrain, Bosnia and Herzegovina, Cape Verde, Chile, Colombia, Costa Rica, Ghana, Gibraltar, Guernsey, Honduras, Indonesia, Israel, Jersey, Kyrgyzstan, Lesotho, Luxembourg, Macau, Madagascar, Malta, Mauritius, Monaco, Montenegro, Morocco, North Macedonia, Peru, Qatar-Financial Centre Free Zone, Russia, Serbia, South Korea, Switzerland, Tunisia, Turkey, United Kingdom and Uruguay. See generally, DLA Piper (n 95).

114 DLA Piper (n 95) 472-3.

115 PDPA (n 57) s. 47.

116 Ibid s. 57.

117 Ibid s. 54.

118 Greenleaf, 'Limitations of Malaysia's Data Protection Bill' (n 101) 1-2.

119 PDPA (n 57) s. 60.

in accordance with the directions of the Minister.[120] The Commissioner, Deputy Commissioner, Assistant Commissioner or any officer or servant of the Commissioner enjoy certain immunities. For example, these officials are exempted from any suit, prosecution or other proceedings for their activities which are carried out in good faith.[121]

7 *Transborder Data Transfer*

The PDPA does not apply to any data processing activities performed outside Malaysia unless there remains an intention that such data would be further processed in Malaysia.[122] It also lays down that the personal data cannot be transferred outside Malaysia unless the place is in the 'whitelist' as determined by the Minister in consultation with the Commissioner.[123]

However, if the Commissioner does not take a strict stand as prescribed, i.e., 'data users take all logical precautions and due care',[124] this may open an unexpected door to data transfers which needs to be closed.[125] Moreover, the Minister is likely to specify the countries (whitelist) to which personal data can be transferred freely.[126] In 2017, the Commissioner issued a 'Public Consultation Paper'[127] seeking feedback from the public on the draft whitelist of countries to which the personal data may be freely transferred without relying on the exemptions as laid down in s. 129(3) of the PDPA.

The stated whitelist comprises the names of numerous countries, including Andorra, Argentina, Australia, Canada, China, Dubai, European Economic Area (EEA) Member States, Faroe Islands, Guernsey, Hong Kong, Isle of Man, Israel, Japan, Jersey, Korea, New Zealand, Philippines, Singapore, Switzerland, Taiwan, UK, Uruguay and the USA.[128] It was further instructed that until the Proposed Order of 2017 is gazetted, the data user shall have to rely on the certain exemptions as set out in s. 129(3) of the PDPA before transferring any data outside Malaysia.[129] Such exemptions include, among others, (a) the data subjects have given their consents to that transfer, (b) the said transfer is essential to perform the contract made between the data user and data subject, (c) the data user has taken reasonable initiatives and care to ensure the compliance of the PDPA and (d) the transfer is crucial for the protection of vital interests of the data subjects.[130]

8 *Enforcement Mechanisms*

The Department of Personal Data Protection (DPDP), led by a Commissioner is entrusted with certain powers to enforce the PDPA. Section 48(2) of the PDPA states that the

---

120 Ibid s. 59.
121 Ibid s. 139.
122 Ibid s. 3(2).
123 Ibid s. 129.
124 Ibid.
125 Greenleaf, 'Limitations of Malaysia's Data Protection Bill' (n 101) 3.
126 Munir, Yasin and Karim (n 69) 224.
127 Personal Data Protection (Transfer of Personal Data to Places Outside Malaysia) Order 2017 (the Proposed Order 2017), (PCP) No. 1/2017. See also Kandiah (n 8) 253.
128 Ibid.
129 Ibid.
130 PDPA (n 57) s. 129(3).

Commissioner shall have the functions to enforce and implement the personal data protection legislation, including the preparation of functional procedures and policies. Under s. 49, the Commissioner shall have the powers to do all things essential, convenient, incidental or consequential to carry on the performance of his functions under PDPA.

Moreover, the Commissioner may exercise numerous other powers, including the issuance of enforcement notice (s.108), refusing of registration for a data user (s. 16(1)(b)), refusing to renew the registration (s. 17(3)), revoking of registration for the data users (s. 18(1)), carrying out inspections on the personal data systems of the data users (s. 101) and publishing reports setting out the recommendations resulting from the inspections users (s. 103).

Similarly, the Commissioner's authorised public officers are also empowered with certain powers, such as conducting investigations of any offence under the PDPA users (s. 112), conducting search and seizure on equipment, systems, electronic data, records and properties of the data user with or without a warrant (ss. 113-114), requiring to produce the books, computers, accounts, electronic data or other records held by data users (s. 121) and arresting any alleged person without a warrant, who has allegedly committed or attempted to commit an offence under the PDPA (s.127).

B *The Shortcomings of the PDPA*

In recent years, enacting data protection law has become one of the major enablers for economic development and upholding a country's image in the world. Malaysia did not waste time to join in the global wave of enacting a comprehensive data protection legislation. There are, however, several shortcomings in the PDPA, particularly, in comparison with the GDPR.

Although the PDPA adopts the traditional approach in defining the term 'personal data', it restricts its application to automated transactions and a few manual transactions only.[131] Moreover, the enactment covers only the personal data in commercial transactions and excludes the public sector. Considering this, Greenleaf remarks, 'within its scope, it will be valuable, but the narrow scope of the Act must always be kept in mind'.[132] The enforcement mechanisms of PDPA are seriously deficient, and unless there exist strict prosecutions of offences, the complainants would become powerless due to the lack of the rights of taking civil litigation.[133]

In another work, Greenleaf portrays the data privacy regime of Malaysia as an inactive one because of several deficits, such as the non-application of the PDPA to the public sectors, the lack of independence of the Commissioner, and falling short of minimum standards in few privacy principles.[134] On a different note, it was further remarked that it would not be easy to achieve the EU adequacy standard for some Asian

---

131 Greenleaf, *Asian Data Privacy Laws* (n 71) 322.

132 Ibid.

133 Ibid 334, 335.

134 Graham Greenleaf, 'Asia's Data Privacy Dilemmas 2014–19: National Divergences, Cross-Border Gridlock' (August 30, 2019). (2019) No 4, Revista Uruguaya de Protección de Datos Personales (Revista PDP), August 2019, 49-73, UNSW Law Research Paper No. 19-103, available at SSRN: https://ssrn.com/abstract=3483794) 64.

countries, such as Taiwan due to the lack of data protection authority, Singapore and Malaysia because of the lack of independence of the data protection authority.[135]

Above all, the PDPA is no doubt a robust and comprehensive data protection legislation but in comparison with the latest data privacy standards, especially, the GDPR, it has several shortcomings, which need to be addressed. Taking account of the gaps, necessity and demand of the day, this article finds the following shortcomings of the PDPA.

i. Compared to the GDPR, the material and territorial scope of the PDPA is limited and needs to be expanded. For example, the PDPA covers only the data processing activities which are processed for commercial purposes, and it is not always easy to determine whether a particular transaction is commercial or not.[136] The PDPA also does not have any application against any government office. In addition, unless further processed in Malaysia, the Act does not apply to the data processed outside the border of the country.

ii. Unlike the GDPR, there is no provision prohibiting an automated decision-making in the PDPA. It is generally presumed that the PDPA shall not pass the EC's adequacy test because of several reasons, and importantly due to the lack of provisions against automated decision-making.[137] The automated decision-making is a provision that allows the data subjects the right not to be subjected to decision-making and profiling based on entirely automatic processing, which generates legal implications concerning them and substantially affects them.[138]

iii. It is noteworthy that the objective against automated decision-making is to impose control over automated decision-making because of the dangers it could potentially pose. For instance, persons of a particular area may be denied of having any credit from any financial institution, not because of their bad history of debt, but as the automation suggests so. Arguably, other than human intervention, automation or computers should not decide whether an individual can get any job, loan or credit facilities.[139] It may be relevant to note that the provision against automated decision-making was incorporated in s. 41 of the draft of PDPA. However, there is no explanation why it has been dropped from the PDPA later.[140]

iv. By use of the Internet protocol addresses (IP address), cookies or radio frequency identification (RFID), coupled with some other exclusive identifiers, personal data can be collected through the servers or the personal profile of an individual or his identity may be exposed. Thus, the latest data protection regulations, for example, the GDPR requires that the data subjects not to be traced by such kinds of tools.[141] The PDPA does not contain any provision like this.

---

135 Ibid 71.

136 PDPA (n 57) s. 4.

137 Munir and Yasin (n 76) 218.

138 GDPR (n 56) arts 21, 22(1), (4) and numerous recitals.

139 Munir and Yasin (n 76) 218.

140 Ibid.

141 GDPR (n 56) recital 30.

iv. Although the PDPA requires the data subject's consent as a lawful basis for data processing, it does not explicitly explain what is meant by consent, and how can consent be taken. Since it is one of the lawful bases for the processing of personal data, consent must be freely given. For consent to be free, it must not be caused by coercion, undue influence, fraud, misrepresentation or mistake, as stated in the Contracts Act 1950. Unlike the PDPA, Article 4 (11) of the GDPR, on the contrary, explains:

> 'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

v. The GDPR obliges the controller and processor to appoint a data protection officer (DPO),[142] specially to handle the following cases, (1) the processing of personal data conducted by a public body other than the courts serving in a judicial capacity and (2) the processing of a large-scale personal data which, by their nature, scope and purposes, requires continuous and systematic monitoring.[143]
Under the GDPR, the DPO performs numerous other works, such as advising the controller, or processor, and employees regarding the processing activities, monitoring the compliance of the Regulation, giving advice on the data protection impact assessment and monitoring its performance, cooperating with the supervisory body and performing as a connecting link for the supervisory body on issues relating to processing, prior consultation.[144]
Thus, it is apparent that the role of a DPO is vitally important, especially for the processing of personal data by a public authority other than the court, and the processing of large-scale personal data that requires continuous and systematic monitoring. The DPO also plays the role of an intermediary as between the data controller, processor and supervisory authority. Notably, there is no provision requiring the appointment of a DPO in the PDPA.

vi. The GDPR requires data controllers to report to the supervisory authority within 72 hours about any data breach incident. The controllers are also bound to inform the data subjects about such breach which is likely to affect their interests significantly.[145]
In PDPA, there is no requirement for data controllers to inform either the supervising authority or the data subjects regarding any occurrence of a breach.

vii Under the GDPR, the data subjects have the right to obtain their personal data which was provided to a controller in a structured and machine-readable format. Moreover, the data subjects can transfer those data to another controller without any interruption from the first controller. This is called the right to data portability, which is genuinely a novel inclusion to the GDPR compared to the previous Directive 95/46/EC. To

---

142 Ibid art 37(1).
143 Ibid art 37(1)(a)(b).
144 Ibid art 39.
145 Ibid art 33(1) and recital 85.

exercise this right, certain conditions must be satisfied - such as the processing shall have to be made with the consent of the data subjects, done by automated means, and the exercise of this right does not adversely affect the freedoms and rights of others.[146] The PDPA does not provide for any right like this at all.

viii. The GDPR imposes a revenue-based fine, the minimum amount of which is €10 million or 2% of annual global turnover,[147] and the maximum is up to €20 million or 4% of annual worldwide turnover, whichever is higher.[148] Additionally, it allows the filing of legal suits for the capture of profits, injunctions and the perpetual prohibition on data processing.[149] On the contrary, the PDPA incorporates both fines and imprisonment. Under the PDPA, the minimum sanctions include a fine not exceeding fifty thousand ringgit or imprisonment for a term not exceeding six months or both.[150] The maximum sanctions include a fine not exceeding five hundred thousand ringgit or imprisonment for a term not exceeding three years or both.[151] Thus, it has become explicit that to compare with the GDPR, the PDPA imposes fewer sanctions for data breaches. The high sanctions have a great utility to compel the data processing companies regarding the compliance of the legal postulates. For example, due to facing the highest GDPR sanctions, the top US giant businesses, such as Google, Facebook, Twitter, Amazon, Microsoft and Apple have been bound to change their privacy policy in compliance with the GDPR.[152] It is assumed that considering the potential of higher sanctions, the Personal Data Protection Act 2012 of Singapore imposes a maximum of $1 million for non-compliance with the Act.[153]

ix. Unlike the previous Directive 95/46/EC, the GDPR introduced purely a new idea, i.e., privacy by design and by default to ensure better protection for privacy and personal data of individuals.[154] It can be argued that privacy can be protected not only by legal norms but also various other techniques, and privacy by design and by default is one of them. This regulatory concept regards privacy as one of the key elements in the design, maintenance and operation of the information systems that belong to every institution.[155] This technique also ensures that by default personal data should not remain accessible to an unspecified number of natural persons without any human interference.[156] Nevertheless, the PDPA does not contain such an innovative mechanism.

---

146 Ibid art 20.

147 Ibid arts 8, 11, 25 to 39; 41(4), 42 and 43.

148 Ibid arts 5, 6, 7, 9; 12 to 22; 44, 49 and 58(2).

149 Ibid arts 83, 84.

150 PDPA (n 57) s. 113(7).

151 Ibid ss 16(4), 18(4) and 130(7).

152 Matt Burgess, 'How Apple, Facebook and Google Are Changing to Comply with GDPR' (24 May 2018) *Wired* <https://www.wired.co.uk/article/gdpr-facebook-google-analytics-apple-amazon-twitter>.

153 *Personal Data Protection Act 2012* (No. 26 of 2012) (Singapore) s. 29(1)(d).

154 GDPR (n 56) art 25.

155 AB Makulilo, 'The GDPR Implications for Data Protection and Privacy Protection in Africa' (2017) 1 *International Journal of Data Protection Officer, Privacy Officer & Privacy Counsel* 15.

156 GDPR (n 56) art 25.

x. Pseudonymisation is another new technique regarding data processing under the GDPR, which ensures the processing of personal data without connecting them to any data subject.[157] The GDPR incorporates this tool to ensure better protection of the personal data of individuals. Under this technique, the data users can process personal data without identifying the data subjects.[158] Therefore, this new tool benefits both the data subjects and the data users. Again, the PDPA does not contain any such mechanism.

It is pertinent to mention that the Malaysian authorities has taken the shortcomings of the PDPA seriously as evinced by the media news. In early November 2019, the former Minister of Communications and Multimedia informed the media that the laws on internet regulation and data protection are under study.[159] In the words of the Minister,

> We had identified there are gaps within the Act and its position when compared to personal data protection legislation in ASEAN member nations, Japan, South Korea and also the European Union's (EU) General Data Protection Regulation (GDPR).[160]

Later, the Ministry of Communications and Multimedia of Malaysia identified several gaps in the PDPA, mostly identical to the above-mentioned shortcomings. Accordingly, the said Ministry issued a document titled 'Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010' giving options to the public to give their comments on 22 issues[161] encompassing the PDPA.[162]

---

157 Ibid art 4(5).

158 Ibid arts 4(5) and 32.

159 Ida Lim, 'Gobind: Laws on Internet Regulation, Personal Data Protection under Study', *Malaymail* (online at 7 November 2019) <https://www.malaymail.com/news/malaysia/2019/10/06/gobind-laws-on-internet-regulation-personal-data-protection-under-study/1797635>.

160 'Minister: Govt to Consult Public on Amendments to Personal Data Protection Law', *Malaymail,* (online at 12 February 2020) <https://www.malaymail.com/news/malaysia/2020/02/12/minister-govt-to-consult-public-on-amendments-to-personal-data-protection-l/1836984>.

161 Comments from the public were solicited for the following shortcomings of the PDPA: (1) direct obligation of the data processor, (2) right to data portability, (3) appointment of DPO, (4) reporting about data breach incidents, (5) clarity in the consent of data subjects, (6) transfer of personal data outside Malaysia, (7) privacy by design, (8) establishing Do Not Call Registry (DNCR), (9) disclosure of the list of the third parties who may use the personal data, (10) civil litigation against the data user, (11) privacy concerns arising from data collection endpoints, (12) application of PDPA over public authorities, (13) cross border data transfer, (14) exemption of business contact information, (15) disclosure of personal data to public regulatory bodies, (16) classification of data users, (17) voluntary registration, (18) application of PDPA on non-commercial processing, (19) application of PDPA on foreign controllers which monitor personal data of the Malaysian citizens, (20) ensuring unsubscribe options from online services, (21) first direct marketing call and (22) processing of personal data in cloud computing.

162 Ministry of Communications and Multimedia, *Review of Personal Data Protection Act 2010* (Public Consultation Paper, No 01/2020, February 2020).

V STRENGTHENING THE PDPA: THE GDPR WAY

To sketch a model of a data privacy legislation for a country with no specific laws or attempting to amend the existing privacy regime is not easy, as there is neither any consensus nor convention indicating the standard for data privacy legislation. For decades, among all data protection models,[163] the EU-based comprehensive model and the US-based sectoral and self-regulatory model are most popular around the world. Although earlier, along with the USA, many countries favoured the sectoral approach to data protection,[164] the scenario has been changed, especially after the introduction of the GDPR on 25 May 2018.

The GDPR now appears to be the gold standard for the global data protection regulations being facilitated by its omnibus legal substance, extensive extraterritorial scope, and together with the influential market powers of the EU.[165] This is evident by the increasing trend of countries enacting or amending relevant domestic legislation across the globe in harmony with the GDPR.

For example, many countries in Europe other than the EU Member States, such as Iceland, Liechtenstein, Norway and Switzerland have changed their data protection laws in line with the GDPR.[166] Besides, numerous other countries, including Africa, Asia, the Caribbean and Latin America are either enacting new data privacy law or amending the previous laws in harmony with the GDPR.[167] Lawyers working with *Ius Laboris* show that there at least 24 countries outside the EU, in which there exist GDPR-related legal developments, verdicts or harmonizing trends.[168]

Thus, the GDPR emerges as one of the most influential data privacy regimes across the globe. In the words of Schwartz, the GDPR appears as the building blocks of the EU and is widely considered as the data privacy law, not only for the EU but also for the entire

---

163 Colin Bennett characterizes four principal models of privacy management - (1) licensing model (Sweden and Denmark, for example, adopted this model), (2) data protection commissioner model (adopting nations, e.g., Canada and New Zealand), (3) registration model (the UK adopts this model while enacting privacy legislation), and (4) self-help and voluntary compliance model (the US adopted this model). Banisar and Davis categorize national privacy frameworks into three central models, e.g., comprehensive model; sectoral model, and self-regulatory model. There can be another two models as well, for example, the coregulatory model and privacy technologies model. See generally, Colin Bennett, 'The Governance of Privacy: New Zealand in Global Perspective', (Presentation at Privacy Awareness Week, Wellington, New Zealand, 5 May 2010) <https://www.colinbennett.ca/Presentations/WellingtonMay2010.pdf>; David Banisar and Simon G Davies, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments' (1999) 18(1) *John Marshall Journal of Computer & Information Law* 1.

164 IJ Lloyd, *Information Technology Law* (Oxford University Press, 2017) 26.

165 Md Toriqul Islam and Mohammad Ershadul Karim, 'Extraterritorial Application of the EU General Data Protection Regulation: An International Law Perspective' (2020) 28(2) *IIUM Law Journal* 531.

166 Nymity, 'Happy Birthday GDPR. At One Year On, What Have We Learned?' (Web Page) <https://www.lexology.com/library/detail.aspx?g=649cd552-7853-4abc-81c6-37af2c8dd415>.

167 Graham Greenleaf and B Cottier, 'Data Privacy Laws and Bills: Growth in Africa, GDPR Influence' (2018) 152 *Privacy Laws & Business International Report* 5.

168 Countries with GDPR-creep legal developments concerning data protection include – Argentina, Bahrain, China, Egypt, Hong Kong, Iraq, Jordan, Kazakhstan, Kuwait, Mexico, Norway, Oman, Peru, Qatar, Russia, Saudi Arabia, United Arab Emirates, United States of America and the United Kingdom. See generally, 'The Impact of the GDPR Outside the EU' (Web Page) <https://theword.iuslaboris.com/hrlaw/whats-new/the-impact-of-the-gdpr-outside-the-eu>.

world.[169] He further remarks that the EU has appeared as a global privacy cop, working unilaterally and applying de facto influence on other States through its market power.[170]

Therefore, this article argues that the Malaysian data protection regime may also be strengthened in light of the GDPR. However, this background may raise several questions encompassing the GDPR, such as what does the GDPR mean? What are its implications on global data protection regulations? How relevant is the GDPR to the PDPA? In the following part, this article discusses the answers to those questions.

A *Introduction to the GDPR*

Operating as a single market of 27 countries, the EU emerged as a major trading partner for many countries of the world. Together with the US and China, the EU is one of the three biggest global actors in worldwide trade.[171] Consequently, the norms, rules and policies of the EU affect the whole world, including Malaysia. The GDPR refers to an EU regulation on the protection of privacy and personal data in the EU and the EEA. The primary objectives of the GDPR are to strengthen the data protection rights of individuals and to develop business opportunities promoting the free flow of data in the EU single market.[172]

The development of the GDPR started from January 2012 with a proposal of the European Commission that was approved on 27 April 2016. Finally, it came into force on 25 May 2018 followed by a long-term dialogue.[173] It is regarded as one of the most comprehensive and far-reaching pieces of Regulation ever enacted as it addresses all possible challenges that people might face regarding their personal data in the digital age. It supersedes the preceding EU Data Directive 95/46/EC offering several changes in almost everything from technology to advertising, and medicine to banking.[174] The long arm of the GDPR reaches to any entity outside the EU dealing with the personal data of EU's inhabitants by offering goods and services or monitoring their behaviours, and the non-compliance thereof may lead to severe consequences.

In the words of Kuner et al., the GDPR shall have global implications by limiting the transnational data transfers, governing the conduct of numerous non-EU institutions, and affecting data protection laws across the world.[175] This statement has become true as

---

169 Paul M Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 *New York University Law Review* 1.

170 Ibid.

171 European Union, 'The Economy' (Web Page) <https://europa.eu/european-union/about-eu/figures/economy_en>.

172 European Council, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)' (2012) Brussels: European Commission <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf>.

173 Gonçalo Almeida Teixeira, Miguel Mira da Silva and Ruben Pereira, 'The Critical Success Factors of GDPR Implementation: A Systematic Literature Review' (2019) *Digital Policy, Regulation and Governance* 404.

174 Alex Hern, 'What Is GDPR and How will it Affect You?' *The Guardian* (Online on 21 May 2018) <https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you>.

175 Christopher Kuner et al, 'The GDPR as a Chance to Break Down Borders' (2017) 7(4) *International Data Privacy Law* 231.

the GDPR has emerged as a clarion call for a unique global data privacy gold standard.[176] This is reflected in the following words of Ursula Gertrud von der Leyen, the President of the European Commission- 'with the GDPR, the EU has set the pattern for the entire world'.[177]

B *Implications of the GDPR*

The recent Report of the UN Special Rapporteur on 'the right to privacy' reveals that the influence of the GDPR is exerted not only on the local legislative measures or extraterritorial application but also for the voluntary compliance of big companies outside the EU, like Microsoft.[178] In mid-2019, top US lawmakers, lobbyists, and business leaders including Mark Zuckerberg (CEO of Facebook), Tim Cook (CEO of Apple) and Sundar Pichai (CEO of Google) called for enacting GDPR-like comprehensive regulation in the USA.[179] Greenleaf remarks, this 'GDPR-creep' is likely to be as crucial as the legislative adoption.[180]

Rustad and Koenig argue that the GDPR has the potential not only to close data privacy wars between two sides of the Atlantic, but also to emerge as the gold standard for global data privacy laws.[181] They also admit the US' roles in global data protection standards. To them, the GDPR imports numerous long-standing US principles of tort into the EU data privacy law, such as wealth-based sentence, deterrence-based fines, collective redress, and empowerment of the data subjects to proceed for public enforcement.[182] The net impact of the GDPR is two-fold – (1) transatlantic privacy convergence and (2) rapid evolution as the global data privacy standard.[183] To support their viewpoints, they mention that countries across the globe, many US States, and most US-based processors introduce policies in conformity with the GDPR.[184] Moreover, based on their survey on global data privacy standards, they also show that the African data privacy standard is usually undeveloped, whereas the approach to the data privacy legislation in Asian countries are mostly inclined to the GDPR.[185] The result of their survey reveals that the

---

176 Giovanni Buttarelli, 'The EU GDPR as a Clarion Call for a New Global Digital Gold Standard' (2016) 6(2) *International Data Privacy Law* 77.

177 European Commission, 'Keynote Speech by President Von Der Leyen at the World Economic Forum' (Web Page) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_102>.

178 Joseph A Cannataci, *Report of the Special Rapporteur on the Right to Privacy to the General Assembly of the United Nations,* Advanced Unedited Report, A/73/45712 (17 October 2018).

179 Elizabeth Schulze, 'The US Wants to Copy Europe's Strict Data Privacy Law – but Only Some of It', *CNBC* (online at 23 May 2019) <https://www.cnbc.com/2019/05/23/gdpr-one-year-on-ceos-politicians-push-for-us-federal-privacy-law.html>.

180 Graham Greenleaf, 'Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi' (2018) *UNSW Law Research Paper*, No 18-56, 3.

181 Michael L Rustad, and Thomas H Koenig, 'Towards a Global Data Privacy Standard' (2018) 71 *Florida Law Review* 366.

182 Ibid 365.

183 Ibid 365, 366.

184 Ibid 366.

185 Ibid 449.

emergence of a 'GDPR-creep' privacy standard is found not only in the 'First World' but also in the 'Second World' and the 'Third World' countries.[186]

C *Relevance of the GDPR to the Malaysian Data Protection Regime*

Generally, the GDPR does not apply to the countries outside the EU unless they process the personal data of the EU residents being within or outside the EU. Therefore, like other non-EU States, Malaysians are not directly bound to comply with the provisions of the GDPR. This backdrop may raise the question – how can the GDPR be relevant for the Malaysian data protection regime?

Generally, the GDPR applies against any establishment in the EU, which processes the personal data of EU individuals regardless of the place of such processing.[187] Further, the GDPR applies against foreign companies, which process personal data of EU residents offering goods or services to them and monitor their behaviour.[188] Finally, it covers data processing activities of any controller or processor having no establishment in the EU but in other places where laws of EU Member States apply by way of public international law.[189] Thus, any entity outside the EU, including Malaysia, may come under the grip of the GDPR if it processes the personal data of the EU residents by offering goods and services or monitor their behaviour.

Furthermore, the GDPR may have a considerable impact on Malaysian business, legal, and policy affairs, as the EU is one of the largest trading partners of Malaysia.[190] In terms of the GDP, Malaysia is the 3rd-biggest economy in the ASEAN and the 3rd-major business partner of the EU in the region.[191] After China and Singapore, the EU is Malaysia's 3rd-major business partner sharing a market of 11.6% of its total trade.[192] Besides, Malaysia became the EU's 23rd global biggest business partner in goods, and accordingly, shared an amount of € 39.8 billion in 2018.[193] Therefore, the implications of GDPR cannot be ignored in the context of Malaysia, but rather the GDPR may play a major role in Malaysian policies, politics and businesses.

D *Global Acceptance and Diffusion of the GDPR*

Despite the above, many authors try to search for the reasons for the worldwide acceptance and diffusion of the GDPR. Working with global acceptance and diffusion of the EU law, Paul M. Schwartz, Anu Bradford, Jack Goldsmith, and Tim Wu have shown that the EU law, particularly the GDPR, has received an unprecedented extension due to three

---

186 Ibid 365, 366.
187 GDPR (n 56) art 3(1).
188 Ibid art 3(2).
189 Ibid art 3(3).
190 Munir and Yasin (n 76) 213.
191 'Countries and Regions' *European Commission* (Web Page) <https://ec.europa.eu/trade/policy/countries-and-regions/countries/malaysia/>.
192 Ibid.
193 Ibid.

factors, such as: (1) the omnibus legal substance,[194] (2) the 'Brussels Effect',[195] and (3) the influential market power.[196] Moreover, the GDPR has been recognised and diffused across the globe by dint of the adequacy decision of the European Commission.

To explain the omnibus legal substance, Paul M. Schwartz remarks that due to the contextual relevance and highness, the EU initiatives toward data protection has always been in the legal talk of the world's leading institutions and individuals. This eventually transplants the GDPR into other privacy protection mechanisms in the world.[197] Businesses' *de facto* adaptation toward EU law lays the foundation for lawmakers' *de jure* enforcement of these laws, which Bradford calls the 'de jure Brussels Effect'.[198] To explain the influential market power, Goldsmith and Wu remarks that the EU's privacy laws are the fourth types of global legislation - not any treaty, like cybercrime convention; not implemented through the architecture of the internet, like the ICANN; not a WTO-regulated trade dispute, like online gambling, but rather, global legislation arising out of the EU's immense market power and it's tenacity for its resident's privacy.[199]

E *The Adequacy Decision*

The GDPR further expands its long arm to countries beyond the EEA area through the adequacy decision. The adequacy decision is the decision of the European Commission as conferred by Article 45 of the GDPR, by which it can evaluate whether a country outside the EEA area provides a similar degree of protection for the personal data of individuals through the domestic law and international commitments.[200] In recent years, it has become a trend across the globe to have adequacy status from the EU. Consequently, many countries, mostly the global trading partners of the EU are either enacting or amending the existing data privacy laws in conformity with the GDPR to obtain the 'adequacy status' from the EU.

Currently, Andorra, Argentina, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, and Uruguay have obtained the complete adequacy decision, and partial findings of adequacy were granted to Canada and the USA.[201] Recently, the EC is working on the adequacy decision on South Korea.[202] Malaysia is neither on the list nor under any consideration.[203]

---

194 Schwartz (n 169) 4.

195 Anu Bradford, 'The Brussels Effect' (2012) 107 *Northwestern University Law Review* 1.

196 Tim Wu and Jack Goldsmith, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press 2006).

197 Schwartz (n 169) 4.

198 Bradford (n 195) 8.

199 Wu and Goldsmith (n 196) 176.

200 European Commission, 'Adequacy Decisions' (Web Page) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>.

201 Ibid.

202 ICO, 'International Transfers' (Web Page) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers#adequacy-decision>.

203 Md Toriqul Islam and Mohammad Ershadul Karim, 'A Brief Historical Account of Global Data Privacy Regulations and the Lessons for Malaysia' (2019) 28(2) *SEJARAH: Journal of the Department of History* 179.

However, there remains an obvious question as to whether there is any way of processing or transferring data from the EU to Malaysia and vice-versa when Malaysia does not fulfil the adequacy requirement. The personal data can still be transferred to Malaysia subject to the fulfilment of appropriate safeguards. Article 46 of the GDPR, for example, renders that in the absence of an adequacy decision under Article 45(3), personal data may also be transferred to the third countries or international institutions only when the controllers or processors have ensured three things for the data subjects - (a) appropriate safeguards, (b) enforceable data subject rights and (c) effective legal remedies.

At the time of enactment of the PDPA, it was generally expected that the PDPA would promote the free flow of data in trade and other joint global initiatives. Given that if Malaysia cannot satisfy the adequacy test, and both the EU and Malaysian businesses are to depend on further contracts for data transfer, then the PDPA is said to be a missed opportunity.[204]

VI CONCLUSION

The existing literature reveals that over time, numerous rights have been recognised across the globe as a natural outcome in major socio-economic and political reforms. Privacy is comparatively a new addition to those rights. It is now settled that the infringement of privacy or a data breach cannot go beyond any challenge. Thus, privacy and data breaches are addressed by multiple legal and regulatory mechanisms. In particular, specific regulations or laws have been made around the world in response to the issues encompassing privacy and data protection. Malaysia has not been lagging in this respect, but rather has joined the elite club of countries with comprehensive data protection laws through the enactment of the PDPA.

Whilst the PDPA is certainly a robust data protection legislation, in comparison with the GDPR, it has shortcomings that need to be addressed. In this article, we have discussed some of the shortcomings and loopholes of the PDPA. In particular, when amending the PDPA, the Malaysian legislature may consider extending the definition of 'personal data' to cover non-commercial transactions. Other issues that may be considered include - widening the scope of the PDPA to cover the government activities, expanding the territorial scope to include both the national and international processors and controllers, adding an explanation to the meaning of 'consent', incorporating provisions for the appointment of DPOs to monitor the data subjects' rights, and inserting some other provisions, such as data breach notification, right to be forgotten and data portability. Further, the Malaysian legislature may also consider revising the provisions of punishment in the light of global best practices and add the pseudonymisation technique for benefitting both the data subjects and the data users.

The PDPA may also incorporate provisions enabling the data subjects to file civil suits for the protection of his or her personal data. Many data protection regimes, such as Singapore,[205] Switzerland,[206] USA, UAE, Portugal, South Africa, Malta, Macau, Chile,

---

[204] Munir and Yasin (n 76) 224.

[205] *Personal Data Protection Act 2012* (n 153) (Singapore) s. 32.

[206] *Federal Act on Data Protection 1992* (235.1) (Switzerland) art 15.

Lesotho, Cape Verde, Bahrain and Uzbekistan incorporate provisions for filing civil suits in regarding the protection of personal data.[207] Moreover, there should be provisions in the PDPA to make data protection authorities answerable to the Federal Parliament of Malaysia. This article concludes by suggesting to the Malaysian legislature to consider the GDPR as a guiding star when it takes steps to amend the PDPA for the purpose of strengthening the data protection regime in Malaysia.

[207] DLA Piper (n 95).