THE MEANING AND SCOPE OF PERSONAL DATA UNDER THE SINGAPORE PERSONAL DATA PROTECTION ACT

It is important to examine and determine the meaning of "personal data" as it is the subject matter of the Singapore Data Protection regime. What constitutes "personal data" determines the scope of the Personal Data Protection Act. Although it is defined under the Act, the experience in other jurisdictions has shown that the elements of that (and other forms of) definition can still give rise to some difficulty in its application to specific cases. In this paper, the authors aim to provide some guidance and recommendations for the interpretation of "personal data" within the context of legislative intent and objective.

Warren B **CHIK**
LLB (National University of Singapore), LLM (Tulane), LLM (UCL);
Associate Dean and Associate Professor of Law,
Singapore Management University School of Law.

PANG Keep Ying Joey
BSc (Economics) (Singapore Management University),
JD (Singapore Management University);
Practice Trainee, Rajah & Tann LLP.

I. Introduction

1 The enactment of the Personal Data Protection Act 2012[1] ("PDPA") on 20 November 2012 marks an important milestone for Singapore's technology law framework. It puts in place a comprehensive set of provisions that provides for baseline standards and requirements for the protection of personal information as well as a regime for the protection of the general public from unwanted voice, fax and text messages. All private organisations are subjected to the data protection obligations under the Act; although it is noteworthy that, unlike some other jurisdictions, public agencies are exempted.[2] The PDPA fills the lacuna in Singapore's data protection regime that prior to the Act comprised only sector-specific legislation and regulations.[3]

1 Act 26 of 2012.

2 Under s 4(1)(*c*) of the Personal Data Protection Act 2012 (Act 26 of 2012), the data protection provisions of the Act will not apply to "any public agency or an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data".

3 However, existing sector-specific legislation and regulations will continue to apply as the Personal Data Protection Act 2012 (Act 26 of 2012) was devised to be a

(*cont'd on the next page*)

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

2 With the data protection provisions of the PDPA[4] due to enter into force on 2 July 2014, there is increased attention and interest on the meaning of the various data protection provisions under the Act. The provisions define the parameters of a private organisation's data protection obligations and the concomitant rights of the individual to the protection of his or her personal information. Central to this inquiry is the concept of "personal data" and what it encompasses, as the data protection obligations under the Act apply only when private organisations are dealing with personal data. In other words, "personal data" is the *subject matter* of the obligations under the personal data protection regime and determines the scope of its application. In contrast, the other exemptions contained within s 4 of the Act, including the public agency exemption, are *exceptions* to the PDPA regime; and the even more limited exceptions pursuant to s 17 and the relevant Schedules to the Act only relate to the consent, access and correction requirements.

II. Overview

3 This article will examine the possible meanings of "personal data" under the PDPA. Section 2(1) of the PDPA provides a statutory definition of "personal data" as "data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access". Nevertheless, different meanings of personal data can arise because of the different interpretive approaches that one can adopt for the various elements of the statutory definition.

4 In this regard, the interpretive approaches to deciphering the meaning of personal data, with reference to the purpose of the Act, will shed light on the various elements that define personal data under s 2(1) of the PDPA. Cases from other countries that have interpreted the same or similar definitions of personal data will also be helpful in predicting the likely scope and coverage of the Act, taking into consideration the political, cultural and socio-economic background of these jurisdictions.

5 In the first part of this article, the authors will identify the general purpose of the statute and consider the policy objectives of the PDPA by examining the purpose provision found in the Act against the backdrop of relevant extrinsic materials such as Parliamentary Reports relating to the passage of the Act, relevant foreign data protection

complementary Act. Section 4(6)(*b*) states that "the provisions of other written law shall prevail to the extent that any provision of Parts III to VI is inconsistent with the provisions of that other written law".

4 Personal Data Protection Act 2012 (Act 26 of 2012) Pts III–VI, ss 11–26.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

statutes that were referred to during the development of the Act as well as the advisory guidelines issued by the Personal Data Protection Commission ("PDPC"),[5] which is the primary enforcement agency of the PDPA. It will be shown that the PDPA seeks to promote three main objectives: (a) to give individuals the right to data protection in a balanced manner that does not impose overly onerous compliance costs on private organisations; (b) to recognise the qualified right of private organisations to collect, use and disclose personal data so as to enhance Singapore's competitiveness and strengthen its position as a trusted business hub; and (c) to develop Singapore into a global data hub by ensuring that Singapore is on par with major economies that have data protection laws so as to facilitate cross-border data transfers.

6 The authors will explore the two possible approaches to the interpretation of personal data in the second part of the article: (a) a broad and expansive approach; or (b) a balance-of-interests approach. The different approaches stem from the two ways in which the purpose of the PDPA could be understood and promoted, and the authors will submit that a broad and expansive approach is to be preferred in order to better meet the purpose and policy objectives of the PDPA identified in part one and to provide conceptual clarity.

7 In the third and final part of this article, the authors will examine in detail the definition of personal data under the PDPA by analysing each element within its meaning under s 2, again by reference to relevant Parliamentary Reports, PDPC guidelines and materials from jurisdictions that were referred to during the development of the Act. This part will examine the meaning of each of the four key elements of "personal data" under the Act, which can be broken down into the following:

(a) "data";

(b) "whether true or not";

(c) "about an individual"; and

(d) "an individual who can be identified" (and the sources of data).

This exercise, using the proposed broad and expansive interpretative approach, is done with a view to clarifying the meaning and parameters of what should constitute personal data under the PDPA in Singapore. Hopefully, this can provide some guidance to the courts, the PDPC and

5 The Personal Data Protection Commission was established as a statutory body on 2 January 2013. See the Personal Data Protection Commission website <http://www.pdpc.gov.sg/personal-data-protection-act> (accessed 7 May 2014).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

the primary stakeholders when the issue of compliance arises within their jurisdiction, mandate and practice respectively.

8 In the appendix to this article, the authors will specifically consider whether Internet protocol addresses ("IP addresses"), telephone numbers and e-mail addresses, should generally be recognised as personal data under the PDPA.

III. Purpose and policy objectives of the PDPA

9 Deciphering the purpose of the PDPA is an important and necessary step to determining the statutory meaning of personal data. Before we look at the objectives of the PDPA, it is apposite to make some brief observations on statutory interpretation and specifically the purposive approach to statutory interpretation.

A. Statutory interpretation in Singapore: The purposive approach

10 The Interpretation Act[6] ("IA") provides guidance for statutory interpretation in Singapore and mandates the purposive interpretation of statutory provisions. Specifically, s 9A(1) of the IA states that:

> In the interpretation of a provision of a written law, an interpretation that would promote the purpose or object underlying the written law (whether that purpose or object is expressly stated in the written law or not) shall be preferred to an interpretation that would not promote that purpose or object.

With reference to the above provision, purposive interpretation hence entails the evaluation of the appropriateness of a statutory interpretation based on whether or not an interpretation would "promote the purpose or object" of the statute in question. Consequently, the determination of the purpose or object of a statute plays a key role in statutory interpretation.

11 As a matter of practice, such determinations can be made from the purpose provision of the statute (if there is one) as well as from the objectives that can be determined from reading the statute as a whole. Secondary materials such as policy and consultation papers as well as parliamentary debates and, in this case, PDPC guidelines can also be "capable of assisting in the ascertainment of the meaning of [a] provision" and due consideration may be given to them under the circumstances stated in s 9A(2) of the IA.

6 Cap 1, 2002 Rev Ed.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

12 In line with s 9A, the Singapore judiciary has made the purposive approach the dominant, if not the paramount approach, to statutory interpretation. Since the enactment of s 9A in 1993, the courts have consistently ruled, on the basis of s 9A, that the purposive approach to statutory interpretation is to be preferred.[7] More recently, this position was affirmed by Sundaresh Menon CJ in the Court of Appeal decision of *Dorsey James Michael v World Sport Group Pte Ltd*[8] ("*Dorsey James Michael*"). In *Dorsey James Michael*, Menon CJ pronounced that "[i]n Singapore, any discussion on statutory interpretation must take place against the backdrop of s 9A of the Interpretation Act".[9] For the avoidance of doubt, the purposive reading of statutory provisions applies even when "on a plain reading, the words of the statutory provisions are unambiguous or do not produce unreasonable or absurd results".[10] The purposive approach is hence to be applied in every instance of statutory interpretation.

13 Adopting a purposive interpretation means that Singaporean courts can, when appropriate, deviate from the literal meaning of the provision examined. In *Comptroller of Income Tax v GE Pacific Pte Ltd*,[11] Yong Pung How CJ stated in the Court of Appeal that "s 9A(1) clearly compels [the court] to put Parliament's intention into effect and allows [the court] to look beyond the words of [the statutory provision concerned]".[12] More recently, V K Rajah JA also stated in *Public Prosecutor v Low Kok Heng*[13] ("*Low Kok Heng*") that a purposive approach "allows the judge the latitude to look beyond the four corners of the statute, should he find it necessary to ascribe a wider or narrower interpretation to its words".[14]

14 However, the court's right to deviate from the literal meaning of provisions is not one without limits. As noted by Rajah JA in *Low Kok Heng*, "the purposive approach stipulated by s 9A is constrained by the parameters set by the literal text of the provision".[15] Hence, taking into consideration the above decisions, it would appear that courts can

7 *Constitutional Reference No 1 of 1995* [1995] 1 SLR(R) 803 at [44]; *Planmarine AG v Maritime and Port Authority of Singapore* [1999] 1 SLR(R) 669 at [22]; *Public Prosecutor v Low Kok Heng* [2007] 4 SLR(R) 183 at [39].

8 [2013] 3 SLR 354.

9 *Dorsey James Michael v World Sport Group Pte Ltd* [2013] 3 SLR 354 at [16].

10 *Dorsey James Michael v World Sport Group Pte Ltd* [2013] 3 SLR 354 at [19] confirming *Planmarine AG v Maritime and Port Authority of Singapore* [1999] 1 SLR(R) 669 at [22].

11 [1994] 2 SLR(R) 948.

12 *Comptroller of Income Tax v GE Pacific Pte Ltd* [1994] 2 SLR(R) 948 at [26].

13 [2007] 4 SLR(R) 183.

14 *Public Prosecutor v Low Kok Heng* [2007] 4 SLR(R) 183 at [30]; Goh Yihan, "Statutory Interpretation in Singapore: 15 Years on from Legislative Reform" (2009) 21 SAcLJ 97 at 109, para 12.

15 *Public Prosecutor v Low Kok Heng* [2007] 4 SLR(R) 183 at [57].

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

deviate from the literal meaning of provisions to "put Parliament's intention into effect" but only if such deviation is not outside the "parameters set by the literal text of the provision"; in other words, where such deviation is within the possible range of meanings that can be accommodated by the literal text of the provision at hand.

15 The determination of the purpose and objective of the statute will also often involve the use of relevant extrinsic materials. As the Court of Appeal observed in *The Seaway*,[16] a "purposive approach to statutory interpretation would invariably involve reference to extrinsic materials that may assist in the interpretation of the statutory provision".[17] Although there was earlier some uncertainty as to whether reference to extrinsic material is allowed if the literal meaning of a provision is clear, this is no longer in doubt after *Low Kok Heng*. In that decision, Rajah JA emphasised that "extrinsic material may be referred to by the courts in statutory interpretation even where the meaning of the provision in issue is clear on its face".[18] All that is required is that courts when admitting the extrinsic materials consider "the desirability of persons being able to rely on the ordinary meaning conveyed by the text of the provision taking into account its context in the written law and the purpose or object underlying the written law"[19] and "the need to avoid prolonging legal or other proceedings without compensating advantage".[20]

16 Finally, by stating that a purposive approach is to be "preferred",[21] the IA arguably permits the use of other methods of interpretation under the right conditions. This view is supported judicially. In *Low Kok Heng*, Rajah JA examined the purposive approach under s 9A(1) of the IA and stated that:[22]

> Other common law principles come into play only when their application coincides with the purpose underlying the written law in question, or alternatively, when ambiguity in that written law persists even after an attempt at purposive interpretation has been properly made.

B. Interpreting purpose provisions

17 Besides the above general observations, there is also the issue of how purpose provisions ought to be interpreted and whether reference

16 [2005] 1 SLR(R) 435.
17 *The Seaway* [2005] 1 SLR(R) 435 at [25].
18 *Public Prosecutor v Low Kok Heng* [2007] 4 SLR(R) 183 at [45].
19 Interpretation Act (Cap 1, 2002 Rev Ed) s 9A(4)(*a*).
20 Interpretation Act (Cap 1, 2002 Rev Ed) s 9A(4)(*b*).
21 Interpretation Act (Cap 1, 2002 Rev Ed) s 9A(1).
22 *Public Prosecutor v Low Kok Heng* [2007] 4 SLR(R) 183 at [41].

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

to extrinsic materials should be allowed when deriving the meaning of such provisions. *Prima facie*, it appears that a purpose provision, like any other statutory provision, ought to be interpreted purposively as mandated under s 9A(1) of the IA. That "there is no blanket rule that a provision must be ambiguous or inconsistent before a purposive approach to statutory interpretation can be taken",[23] can also be taken as further support of the position that purpose provisions ought to be purposively interpreted.

18 However, the purposive interpretation of purpose provisions can be problematic in practice. To purposively interpret a provision, a court would typically employ a three-step approach. First, the court would determine the general purpose of the statute and, if possible, the purpose of the specific provision at hand, by referring to the purpose provision and relevant extrinsic materials, such as the parliamentary speech by the Minister moving the Bill containing the provision during the Bill's second reading. Secondly, the court would then consider the range of meanings supportable by the text of the provision. Lastly, the court would decide on an interpretation by ensuring that the chosen interpretation best promotes the predetermined purpose of the statute. However, applying this approach to the interpretation of a purpose provision would be problematic as this would be a self-referencing and tautological exercise. Given that the purpose of a statute needs to be determined before a purposive approach can be utilised and that the purpose provision is meant to explain the objective of the statute, it is difficult to see how the purpose provision can be concomitantly subjected to the purposive approach to statutory interpretation. Moreover, that will mean that secondary material could in fact be just as, if not more, important in interpreting a statute than the purpose provisions which (unlike the former) forms part of the written law. It is thus submitted that the purposive approach should thus not be applicable for the interpretation of purpose provisions.

19 Instead it is submitted that purpose provisions ought to be interpreted in one of two ways. First, where there are no relevant and admissible extrinsic materials available, the literal meaning of the purpose provision should determine the purpose of the statute. Alternatively, where there are relevant and admissible extrinsic materials, the purpose should then be determined by considering such extrinsic materials against the literal meaning of the purpose provision. Consideration of the extrinsic materials will thus expand or narrow the literal meaning of the purpose provision, subject to the limit that it does not go beyond the parameters set by the literal text of the purpose provision. A purpose provision tends to constitute generalised statements

23 *Planmarine AG v Maritime and Port Authority of Singapore* [1999] 1 SLR(R) 669 at [22].

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

of its objectives rather than to serve as more specific guidance for the interpretation of specific provisions. Nevertheless, the purpose provision is important as it is that part of the statute ("written law") that sets out the objective of the Act and that should not be overridden by secondary materials, which should serve merely as affirming or assisting in the interpretation of specific provisions. It is also there as a reminder to any person interpreting the Act of its main objectives.

C. Purpose of the PDPA

(1) The purpose provision of the PDPA

20 Determining the objective of the PDPA is vital as the purpose so determined will provide guidance on interpreting the other provisions of the Act. In particular, it will be useful in determining what is a fair balance of the interests stated therein in cases where more than one stakeholder and a variety of interests are enunciated. It will also be instructive on the overarching goal of the statute. Consequently, it will also be useful when applying the objective-subjective "reasonable person" test in various provisions of the Act (such as the general compliance rule with respect to the protection of personal data contained in s 11), and when considering what would be an acceptable exception or an appropriate exemption to the general obligations for organisations dealing with personal data that are contained in the Act. Given that a purpose provision exists in the PDPA, the interpretation of this provision would provide the objective for the PDPA. Specifically, s 3 of the PDPA states that:

> The purpose of this Act is to govern the collection, use and disclosure of personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

21 *Prima facie*, two observations can be made from the above. First, s 3 defines the scope of the PDPA as covering only issues that regulate the collection, use and disclosure of personal data by private organisations. Second and more importantly, these regulations are to be guided by two main parameters. These parameters include the right of the individual to protect their personal data and the need of private organisations to collect, use and disclose personal data (but subject to purposes that a reasonable person would consider appropriate in the circumstances).

22 In the subsequent paragraphs, the rights of both the individual and organisations will be referred to. Although s 3 only refers to an organisation's "need", the fact is that the extent of the individual's "right" is curbed by the organisation's "need" and as such they are but two sides

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

of the same coin. Both rights are not absolute, but rather, qualified by the test of reasonableness.

(2) Right of the individual to protect their personal data

23 The PDPA's recognition of "the right of individuals to protect their personal data"[24] means that for the first time, the individual is conferred the right to personal data protection generally. However, this right is not without limits. As made clear by s 3 of the PDPA, the individual's personal data will not be protected when the personal data is collected, used or disclosed by private organisations for purposes deemed appropriate by a reasonable person in the circumstances. Compliance costs to organisations also affect the extent of protection accorded as Parliament made clear that the PDPA takes "the approach of protecting individuals' personal data without imposing overly-onerous requirements on organisations".[25]

24 This right also appears to be a discrete and more focused right to data protection as opposed to being a more fundamental right to privacy (as a human right) or data privacy.

25 First, this right to data protection is not analogous to, or derived from, the right to privacy. Although all the jurisdictions referenced[26] ("referenced jurisdictions") during the development of the PDPA by the Ministry of Communications and Information ("MCI") take the view that the right to data protection is analogous to, or at least derived in part from, the right of privacy; this was not reflected in the PDPA. The concept of privacy does not feature in any of the PDPA's data protection provisions. That privacy forms the basis of the right to data protection was also not mentioned in the parliamentary speeches of the Minister for Information, Communications and the Arts ("Minister") who moved the Bill at its second reading.

26 Further support for the view that the right of data protection is distinct from the right to privacy can also be found by examining the PDPA's adaptation of the purpose provision from Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA").[27]

24 Personal Data Protection Act 2012 (Act 26 of 2012) s 3.

25 *Singapore Parliamentary Debates, Official Report* (15 October 2012) "Personal Data Protection Bill" vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Communications and Information). The Ministry for Information, Communications and the Arts became the Ministry of Communications and Information after a restructuring exercise on 1 November 2012.

26 Jurisdictions that were referenced during the development of the Personal Data Protection Act 2012 (Act 26 of 2012) include Australia, Canada, the European Union, Hong Kong, New Zealand and the UK.

27 RSC 2000, c 5 (Can) s 3.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

Although the PDPA's purpose provision shares an identical structure with its counterpart in the PIPEDA,[28] the PDPA adaptation of the purpose provision specifically excludes mention that it "recognises the right of privacy of individuals".[29] Instead, the PDPA states that it recognises "the right to individuals to protect their personal data". Consequently, it is submitted that the "right of individuals to protect their personal data"[30] ought to be limited to what is provided under the PDPA provisions and not construed wider as incorporating protection for privacy.

27 Besides, reading the right to data protection as limited to the PDPA provisions ensures greater compatibility with Singapore's current laws. As Singapore has hitherto not recognised an individual's right to privacy in statute and the common law, having a right to data protection informed by PDPA provisions as opposed to one flowing from privacy would sit better with the current laws of Singapore. This view also reflects Parliament's intentions. At the second reading of the Personal Data Protection Bill, the Minister stated that the PDPA "does not seek to change any right or obligation conferred by or imposed under the common law".[31] Hence, since no general right to privacy exists in Singapore and the PDPA has not indirectly created this right, the right to data protection therefore ought to be defined solely by the PDPA provisions.

28 Secondly, the right to data protection under the PDPA is also not a fundamental right. In the European Union ("EU"), the right to data protection is a fundamental right enshrined in Art 8 of the EU's Charter of Fundamental Rights[32] and statutes incompatible with this fundamental right would be struck down by the European Court of Justice. In contrast, the PDPA yields to conflicting statutes. Specifically, s 4(6)(*b*) of the PDPA provides that:

> … the provisions of other written law shall prevail to the extent that any provision of Parts III to VI [the data protection provisions] is inconsistent with the provisions of that other written law.

The right to data protection under the PDPA is thus neither a fundamental one nor based upon one.

---

28 Personal Information Protection and Electronic Documents Act (RSC 2000, c 5) (Can) s 3.

29 Personal Information Protection and Electronic Documents Act (RSC 2000, c 5) (Can) s 3.

30 Personal Data Protection Act 2012 (Act 26 of 2012) s 3.

31 *Singapore Parliamentary Debates, Official Report* (15 October 2012) "Personal Data Protection Bill" vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Communications and Information).

32 Charter of Fundamental Rights of the European Union (18 December 2000).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

(3) Right of private organisations to collect, use or disclose personal data

29 The right of private organisations to collect, use or disclose personal data is also a qualified one. As observed in s 3 of the PDPA, this right is subject to the purpose being considered as appropriate by a reasonable person under the circumstances. In this regard, the curtailment of this right is directly reflective of the tension between an individual's right to data protection and an organisation's right to data exploitation.

30 This objective-subjective test – the objective person in a subjective set of circumstances – is a neutral test and in fact serves to define the line between the "rights" of individuals to the protection of their personal data and of organisations to exploit them. Just as an individual's right to data protection may not extend to a situation where it imposes too onerous a cost on private organisations, the right of the private organisations to exploit personal data is constrained to the extent that it violates the right of individuals' to protection of their personal data to an unreasonable degree.

31 Section 11 of the PDPA reinforces the premise that the *primary* duty is on the organisation to comply with the Act. Subsection 1 states that the organisation must be the one to consider whether their practices are what a reasonable person would consider appropriate under the circumstances. Subsection 2 further stipulates that "[a]n organisation is responsible for personal data in its possession or under its control".

32 By recognising a qualified right of private organisations to exploit personal data, Parliament's intention behind the promulgation of this right appears to arise from three considerations.

33 The first consideration is focused on the compliance costs arising from the PDPA and the effect that such costs will have on organisations' (in particular, the small and medium enterprises ("SMEs")) ability to continue to function effectively and in a sustainable manner. As the Minister noted in reply to queries on compliance costs during the second reading of the Bill, "the issue of compliance costs, especially for SMEs … is a key consideration … in developing this Bill" and that efforts "have been sought to mitigate compliance costs for businesses where possible".[33]

33 *Singapore Parliamentary Debates, Official Report* (15 October 2012) "Personal Data Protection Bill" vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Communications and Information).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

34 That the PDPC has moved to actively help SMEs cope with the PDPA also further supports this consideration. In May 2013, the PDPC announced that together with SPRING Singapore, a statutory board under the Singapore Ministry of Trade and Industry responsible for helping Singapore enterprises, it "will work closely with SME Centres to reach out to their members and to support their business advisors in helping the SMEs on personal data protection matters".[34] The PDPC is also working closely with the Workforce Development Agency, a statutory board under the Singapore Ministry of Manpower responsible for promoting work skills training, "to incorporate data protection competencies into existing training frameworks".[35] All these measures are designed to help SMEs meet their obligations under the PDPA by ensuring that their data protection officers have the necessary capabilities and knowledge of the PDPA for practical compliance.

35 Secondly, Parliament also considered the broader issue of Singapore's competitiveness as a business destination when it decided to recognise this qualified right to exploit personal data. Specifically, the Minister considered that a "data protection regime can help promote business innovation and enhance competitiveness" and that personal data, "if appropriately used, can lead to better services and products that help local businesses become more competitive".[36] It thus follows that the PDPA "will also enhance Singapore's competitiveness and strengthen [Singapore's] position as a trusted business hub".[37]

36 Lastly, it is clear that Parliament intends for the PDPA to play a key role in developing Singapore into a global data hub. As noted by the Minister during the second reading of the Bill, the PDPA supports "Singapore's development as a global data hub by providing a conducive environment for global data management industries, such as cloud computing and business analytics, to operate in Singapore".[38] More specifically, Parliament intends for the PDPA to facilitate this development by using the PDPA to "put Singapore on par with the

34 Personal Data Protection Commission, "PDPC Prepares Businesses for the Personal Data Protection Act" (15 May 2013).

35 *Singapore Parliamentary Debates, Official Report* (15 October 2012) "Personal Data Protection Bill" vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Communications and Information).

36 *Singapore Parliamentary Debates, Official Report* (15 October 2012) "Personal Data Protection Bill" vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Communications and Information).

37 *Singapore Parliamentary Debates, Official Report* (15 October 2012) "Personal Data Protection Bill" vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Communications and Information).

38 *Singapore Parliamentary Debates, Official Report* (15 October 2012) "Personal Data Protection Bill" vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Communications and Information).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

growing list of countries that have enacted data protection laws and facilitate cross-border transfers of data".[39]

(4) The three objectives of the PDPA

37 Having examined the purpose provision and its component parts alongside relevant extrinsic materials, one can conclude that the PDPA has *three* main objectives. First, the PDPA recognises the qualified right of individuals to data protection. However, the content of this right will be defined by the data protection provisions[40] under the PDPA and does not flow from the right of privacy. This right is also not a fundamental right and its ambit will be limited to the extent that it would not make working with personal data too onerous for private organisations.

38 Second, the PDPA recognises the need of private organisations to collect, use and disclose personal data and has provided private organisations with a qualified right to do so under a "principle-based and technology-neutral approach".[41] Besides ensuring that such a qualified right does not overreach and render the individual's right to data protection meaningless, the PDPA also seeks to streamline and strengthen Singapore's businesses and her competitiveness through the granting of this qualified right, both domestically and globally, so as to facilitate transactions which would have otherwise bypassed Singapore due to the lack of a data protection framework.

39 Third, the PDPA supports the development of Singapore into a global data hub. To do so, where it is possible, the PDPA seeks to be on par with the data protection regimes of other countries, especially those of major economies such as the jurisdictions referenced by the MCI during the development of the PDPA. A robust data protection regime will attract data management industries to the island and facilitate cross-border transfers of data to and from Singapore.

IV. Two possible approaches to defining the scope of personal data

40 From the above general purposes of the PDPA, it would appear that the purposive interpretation of personal data to define its scope of

39 *Singapore Parliamentary Debates, Official Report* (15 October 2012) "Personal Data Protection Bill" vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Communications and Information).

40 Personal Data Protection Act 2012 (Act 26 of 2012) Pts III–VI, ss 11–26.

41 *Singapore Parliamentary Debates, Official Report* (15 October 2012) "Personal Data Protection Bill" vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Communications and Information).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

coverage could take one of two general approaches: a balance-of-interests approach or a broad and expansive approach.

A. Balance-of-interests approach

41 First, one could employ a balance-of-interests approach that construes personal data contextually; that is, what constitutes personal data will be determined by considering whether such a reading promotes the right of individuals to data protection while not making compliance overly onerous for private organisations working with personal data. Arguably, this approach is in line with the general purposes of the PDPA under s 3,[42] as it promotes the right of individuals to data protection to the extent that it does not overburden private organisations when it comes to compliance.

42 Adopting this approach would also put Singapore on par with some of the jurisdictions referenced by the PDPA. Specifically, Hong Kong and Australia have in their data protection legislations the requirement that identification of personal data should be conducted "practicably" and "reasonably" respectively. For Hong Kong, among other requirements, data is personal data if "it is practicable for the identity of the individual to be directly or indirectly ascertained"[43] from the data, with "practicable" further defined as "reasonably practicable".[44]

43 As for Australia, its federal and state legislations have defined personal information, the analogue to personal data under the PDPA, as information about, *inter alia*, an individual whose identity "can reasonably be ascertained, from the information or opinion".[45] Judicial pronouncements on what is "reasonable" in Australia appear to be guided by factual considerations,[46] with special attention given to the circumstances involved in each case. Even though this part of the provision was recently changed to "reasonably identifiable" on 12 March 2014 following the passage of a law reform Bill by the Australian Parliament on 29 November 2012,[47] this does not substantially change

42 Personal Data Protection Act 2012 (Act 26 of 2012) s 3.

43 Personal Data (Privacy) Ordinance 1995 (Cap 486) (Hong Kong) s 2(1)(b).

44 Personal Data (Privacy) Ordinance 1995 (Cap 486) (Hong Kong) s 2(1).

45 Privacy Act 1988 (Act No 119 of 1988) (Cth) s 6; Cabinet Administrative Instruction No 1 of 1989 (SA); Privacy and Personal Information Act 1998 (Act 133 of 1998) (NSW) s 4; Information Privacy Act 2000 (No 98 of 2000) (Vic) s 3; Information Act 2002 (NT) s 3; Personal Information Protection Act 2004 (No 46 of 2004) (Tas) s 3; Information Privacy Bill 2007 (Bill No 193) (WA) s 6; Information Privacy Act 2009 (Qld) s 12.

46 Mark Burdon & Paul Telford, "The Conceptual Basis of Personal Information in Australian Privacy Law" [2010] MurUEJL 1 at 18.

47 Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Act No 197 of 2012) (Cth).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

the above analysis. As the main amendment is the removal of the words "from the information or opinion", the consideration for reasonableness continues to apply in the amended Australian Privacy Act albeit in a different and much more contextual form.

B. Broad and expansive approach

44 Alternatively, a broad and expansive approach that confers a wide meaning to personal data could be adopted. *Prima facie*, this approach more strongly affirms the right of individuals to data protection under the PDPA but will entail greater responsibility for organisations that will lead to greater compliance costs.

45 However, it should be noted that although legal responsibility for personal data would indeed expand under a broader definition, the wide statutory exemptions under the PDPA nevertheless still apply to counterbalance and lighten the burden on organisations. As noted previously, s 4 limits the application of the Act by generous exclusions including the exemption of various forms of organisations, public agents, data intermediaries and some individuals. The Act also does not apply to certain types of information (*ie*, business contact information) and the duration of protection is limited. Other exemptions under the Schedules to the PDPA (read with s 17 of the Act) also waive the need for private organisations that are still subject to the provisions of the Act to comply with certain data protection obligations under certain situations. Specifically, the Second to Fourth Scheds to the PDPA respectively permit the collection,[48] use[49] and disclosure[50] of personal data without the consent of the individual under certain circumstances, while the Fifth and Sixth Scheds provide exceptions to the right of individuals to access[51] and correct[52] personal data held by an organisation. In other words, these measures already provide the counterweight in favour of organisations, and as such, a broader and more expansive interpretation of "personal data" in favour of individuals is justified and equitable.

46 "Reasonableness" requirements under the PDPA also help to further prevent compliance costs and restrictions from becoming unduly onerous. Section 11(1) states that "[i]n meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances". If that threshold is met, then according to s 3, the organisation would have

48 Personal Data Protection Act 2012 (Act 26 of 2012) Second Sched.
49 Personal Data Protection Act 2012 (Act 26 of 2012) Third Sched.
50 Personal Data Protection Act 2012 (Act 26 of 2012) Fourth Sched.
51 Personal Data Protection Act 2012 (Act 26 of 2012) Fifth Sched.
52 Personal Data Protection Act 2012 (Act 26 of 2012) Sixth Sched.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

met its responsibility under the Act. Specific provisions under the Act also extend this "reasonableness" test to different situations or obligations. For example, to ameliorate the harshness of the consent requirement, an organisation is deemed to have obtained the consent of an individual if the individual provides the personal data voluntary and it is "reasonable that the individual would voluntarily provide the data".[53] Similarly, organisations need only comply with individuals' request to access their personal data on an "as soon as reasonably possible" basis.[54] Organisations could also turn down requests to correct personal data by individuals if it is "satisfied on reasonable ground that a correction should not be made".[55] Furthermore, organisations would only need to make "reasonable effort to ensure that personal data … is accurate and complete"[56] and protect personal data using "reasonable security arrangements".[57] Organisations would also only be made to cease retention of personal data when it is "reasonable to assume that"[58] the business and legal purposes for which the data is collected are no longer being served.

47 This approach is also supported by some jurisdictions referenced by the PDPA. In Canada, the federal judiciary has on multiple occasions[59] mandated that personal information, the analogue of personal data under the PDPA, should be accorded a broad and expansive interpretation.

48 Personal data is also widely construed in the EU and UK. As noted by the Article 29 Working Party[60] in its opinion on the concept of personal data ("WP136"),[61] the "definition [of personal data] reflects the intention of the European lawmaker for a wide notion of 'personal data', maintained throughout the legislative process".[62] Judicially, the European Court of Justice ("ECJ") has also taken a broad view of personal data.

53 Personal Data Protection Act 2012 (Act 26 of 2012) s 15(1).
54 Personal Data Protection Act 2012 (Act 26 of 2012) s 21(1).
55 Personal Data Protection Act 2012 (Act 26 of 2012) s 22(2).
56 Personal Data Protection Act 2012 (Act 26 of 2012) s 23.
57 Personal Data Protection Act 2012 (Act 26 of 2012) s 24.
58 Personal Data Protection Act 2012 (Act 26 of 2012) s 25.
59 *Dagg v Canada (Minister of Finance)* [1997] 2 SCR 403 at [68] (dissenting judgment); *Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board)* 2006 FCA 157; *Canada (Information Commissioner) v Canada (Commissioner of the Royal Canadian Mounted Police)* [2003] 1 SCR 66; 2003 SCC 8 at [23].
60 This is a working party set up under Art 29 of the European Union data protection directive, Directive 95/46/EC of the European Parliament and of the Council (24 October 1995) (protection of individuals with regard to the processing of personal data and on the free movement of such data).
61 Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data, WP 136* (20 June 2007).
62 Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data, WP 136* (20 June 2007) at p 4.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

In the 2003 Swedish case of *Bodil Lindqvist v Aklagarkammaren i Jonkoping*,[63] the ECJ took a broad view of personal data and held that information about a person's working conditions and hobbies are personal data.[64]

49 The UK Information Commissioner also followed the EU's approach by taking a wide reading of personal data even though it continues to face some problems in reconciling this broad reading with the decision in *Durant v Financial Services Authority*[65] ("*Durant*"). In *Durant*, the English Court of Appeal adopted a decidedly narrower interpretation of personal data by limiting personal data to "information that affects [one's] privacy".[66] Despite the fact that *Durant* had been followed in subsequent cases and remains as "good" law, two developments since then that seem to confine *Durant* to the unique facts of that case are instructive. First, the UK Information Commissioner subsequently issued guidance on personal data in 2007 that purports to support both a broad reading of personal data and the decision in *Durant*;[67] but it has been noted that the guidance is in substance an affirmation of the broad approach as adopted by the Article 29 Working Party.[68] Second, in the Court of Appeal's latest decision dealing with the interpretation of personal data, *Edem v The Information Commissioner & Financial Services Authority*[69] ("*Edem*"), the judges distinguished *Durant* and seemed to relegate the effect of that decision to a much narrower situation. This will be considered in more detail later in this article.

C. Justifying the adoption of the broad and expansive approach

50 As noted in the previous two sections, two possible approaches, that are attractive for different reasons, are available for the interpretation of personal data under the PDPA. While both approaches will put Singapore on par with the data protection laws of major economies, since some major economies support either of the approaches,[70] it is submitted that the broad and expansive approach to

63 (C-101/01) [2003] ECR I-4989.

64 *Bodil Lindqvist v Aklagarkammaren i Jonkoping* (C-101/01) [2003] ECR I-4989 at [24].

65 [2003] EWCA Civ 1746.

66 *Durant v Financial Services Authority* [2003] EWCA Civ 1746 at [28], *per* Auld LJ.

67 United Kingdom, Information Commissioner's Office, *Data Protection Technical Guidance – Determining What is Personal Data* (21 August 2007).

68 Christopher Millard & Peter Church, "UK – ICO Guidance on Personal Data: Clarification or Further Confusion?" (Linklaters, 1 November 2007).

69 [2014] EWCA Civ 92.

70 The balance-of-interests approach appears to be supported by Australia, Hong Kong and New Zealand, while the broad and expansive approach has found support in Canada, the European Union and the UK.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

the interpretation of personal data ought to be taken. Specifically, the broad and expansive approach should be preferred for three reasons.

51 First, the broad and expansive approach to the interpretation of personal data should be preferred as it was specifically intended by Parliament. During the second reading of the Bill, the Minister noted, in reply to concerns that the definition of personal data was too broad and vague, that "it is necessary for the definition to be sufficiently broad to allow the Bill to apply to differing circumstances".[71] The broad interpretation of personal data also appears to be supported by the PDPC, which lists in its advisory guidelines that the definition of personal data "is not intended to be narrowly construed and covers all types of data from which an individual can be identified".[72] Such an approach will also be consistent with a purposive interpretation of the definition of "personal data" under s 2, rather than a literal interpretation, especially in relation to the interpretation of the phrase "[data] about an individual".

52 Secondly, a broad and expansive approach to the interpretation of personal data also sits better with the scheme of the PDPA. As observed earlier in this article, the PDPA has built-in exemptions and "reasonableness" requirements to prevent organisations from being overburdened by data protection obligations. A broad reading of personal data would thus sit well with the current scheme of the PDPA by complementing the above mechanisms with its greater recognition of the individual's right to data protection to counterbalance the generous exceptions. It will also be fair and equitable to do so.

53 Lastly, a broad and expansive view of personal data provides greater clarity to the concept of personal data. The broad and expansive approach offers a conceptually neater view of personal data as it determines personal data solely on the identifiability of the data at hand. In contrast, the balance-of-interests approach to the determination of personal data is more complicated, as it often requires additional considerations of "reasonableness" or "practicability", considerations which are highly contextual and circumstantial in nature (and that may be duplicitous, given the tests that are already built into many of the obligations under the Act). Adopting a broad and expansive interpretation of personal data, which provides personal data with a more certain meaning, will actually make it easier for organisations to comply with the PDPA by reducing ambiguities over its definition.

---

71 *Singapore Parliamentary Debates, Official Report* (15 October 2012) "Personal Data Protection Bill" vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Communications and Information).

72 Personal Data Protection Commission, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (24 September 2013) at para 5.2.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

V. Statutory definition of personal data under the PDPA

54 Having explored the general purposes of the PDPA and identified the specific approach that should be taken for the purposive interpretation of personal data, we will now examine the statutory definition of personal data as provided under the PDPA. Specifically, the definition of personal data is provided under s 2 of the PDPA, which states that:

> 'personal data' means data, whether true or not, about an individual who can be identified –
>
> (*a*) from that data; or
>
> (*b*) from that data and other information to which the organisation has or is likely to have access …

A. Definitional similarities and differences with other jurisdictions

55 The definition of personal data under the PDPA is very similar to its counterpart under the UK Data Protection Act 1998[73] ("DPA"). That this is the case is not unsurprising as the UK was one of the jurisdictions referenced during the development of the PDPA. Juxtaposing the PDPA with the DPA, the PDPA appears to have adopted the DPA's structure in its definition of personal data but made some modifications. Specifically, s 1(1) of the DPA states that:

> 'personal data' means data which relate to a living individual who can be identified –
>
> (a) from those data, or
>
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual …

56 *Prima facie*, three main differences can be observed between the statutory definition of the PDPA and DPA. First, the PDPA did away with the requirement of a "living individual" in the DPA, suggesting that personal data could include that of deceased individuals for limited protection. This reading is borne out by s 4(4)(*b*) of the PDPA, which states that the provisions on disclosure and s 24 on the protection of personal data applies to "personal data about an individual who has been dead for 10 years or fewer".[74]

73 c 29.

74 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(4)(*b*).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

57 Secondly, the PDPA includes the additional qualifier of "whether true or not" to state that the veracity of information is an irrelevant consideration and that identification of individuals by the information involved remains the crux to determining personal data. This modification is probably inspired by Australia, being the only referenced jurisdiction that includes these words,[75] and is consistent with the broad and expansive view of personal data supported by the PDPC.[76] Further, this qualifier arguably allows the possible admission of expressions of opinion as personal data under the PDPA. Even though the PDPA departs from the DPA by not specifying "expression of opinion"[77] as admissible, expression of opinion could arguably still be admissible since the truth or otherwise of a statement is irrelevant. An opinion can fall anywhere along a scale between absolute truth on the one side and falsity on the other, being to some extent subjective in nature.

58 Lastly, the PDPA also uses the associative term "about" as opposed to "relate to" in its definition of personal data. The use of "about" in the statutory definition of personal data is found in several jurisdictions including those referenced by the PDPA such as Australia, Canada and New Zealand. Specifically, it has been noted that Australian[78] and New Zealand[79] jurisprudence has taken the view that "about" is more restrictive than "relate to" in terms of how data could be associated with an individual. If the PDPA took this view into consideration in its use of "about" in the definition, then this would imply a more restrictive scope of information that could be associated with individuals in order to form personal data. However, this view is inconsistent with a broad reading of personal data and arguably[80] the term "about" should be synonymous with "relate to"[81] in the local context.

B. Elements of personal data under the PDPA

59 Four main elements comprise the definition of "personal data" under s 2 of the PDPA. These four elements, which are (a) "data"; (b) "whether true or not"; (c) "about an individual"; and (d) "an

75 Privacy Act 1988 (Act No 119 of 1988) (Cth) s 6.
76 Personal Data Protection Commission, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (24 September 2013) at paras 5.7–5.8.
77 Data Protection Act 1998 (c 29) (UK) s 1(1).
78 Mark Burdon & Paul Telford, "The Conceptual Basis of Personal Information in Australian Privacy Law" [2010] MurUEJL 1 at 13.
79 *CBN v McKenzie Associates* [2004] NZHRRT 48 at [39].
80 For further submissions on why the change of phasing from "relate to" to "about" is more semantic than material, see paras 77–90 below.
81 Personal Data Protection Commission, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (24 September 2013) at para 5.3.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

individual who can be identified" (from that data and/or other information that the organisation has or is likely to have access to), will be examined in the following sections.

(1) "Data"

60 The definition of "data" is important as it is the subject matter of the statutory protection under the data protection regime of the PDPA. Consequently, how "data" is to be construed will narrow or broaden the scope of personal data and the applicability of the PDPA.

(a) Preliminary observations of "data" under the PDPA

61 "Data" appears to include information recorded in both electronic and non-electronic form. Although a statutory definition for personal data is provided under the PDPA, the definition of "data" is absent from the Act. The PDPC has also thus far not provided guidance on the constitution of "data". Parliament has, however, shed some light on this issue. During the second reading of the Bill, the Minister stated that "[t]he definition [of personal data] also covers personal data recorded in both electronic and non-electronic formats".[82] Referencing the above, it would thus follow that "data" would cover information, written or otherwise recorded (*eg*, audio/visual), in manual or electronic/digital format. There are also no other qualifiers unlike in some jurisdictions, which will be elaborated in the paragraphs below.

(b) Cross-jurisdictional comparisons

62 Compared with some of the referenced jurisdictions, "data" under the PDPA has a broader meaning and is consistent with a broad and expansive reading of personal data. Under the UK DPA, from which Malaysia's Personal Data Protection Act 2010[83] took substantial guidance, information is only "data" when the information is processed[84] or recorded with the intention to be processed[85] by "equipment operating automatically in response to instructions given for that purpose" or when the information "is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system".[86] In contrast, "data" under the PDPA is broader in scope as

82 *Singapore Parliamentary Debates, Official Report* (15 October 2012) "Personal Data Protection Bill" vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Communications and Information).

83 Personal Data Protection Act 2010 (No 709 of 2010) (M'sia) s 4. This Act entered into immediate effect after it was gazetted on 15 November 2013.

84 Data Protection Act 1998 (c 29) (UK) s 1(1)(a).

85 Data Protection Act 1998 (c 29) (UK) s 1(1)(b).

86 Data Protection Act 1998 (c 29) (UK) s 1(1)(c).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

the means and reason for recording the information is unstated and is hence not a requirement.

63 Hong Kong's Personal Data (Privacy) Ordinance 1995[87] ("PDPO") also has a more restricted view. Under the PDPO, "data" is taken to mean "any representation of information (including an expression of opinion) in any document, and includes a personal identifier".[88] "Data" under the PDPA is thus also broader in scope as it does not require a "personal identifier".

64 Further, this wide and expansive view of "data" under the PDPA is also supported by some of the referenced jurisdictions, notably the EU, Australia and Canada. As noted by the Article 29 Working Group of the EU Data Protection Directive, "data" can include "information available in whatever form, be it alphabetical, numerical, graphical, photographical or acoustic".[89] Implicit in this understanding of "data" is that all that is required is for information to be recorded regardless of its form, which is an understanding that is consistent with "data" under the PDPA.

65 In Australia, although the Privacy Act 1988[90] states that "personal information", the analogue to personal data under the PDPA, includes information "whether recorded in a material form or not", the Australian judiciary has adjudged this as meaning that information should still be recorded albeit not always in material form. Specifically, the Australian Court of Appeal held that:[91]

> It is almost impossible to conceive how almost all those [data protection] sections … could operate in practice if they were intended to apply to information in the minds of employees acquired by direct visual or aural experience and never recorded in any manner.

66 This understanding and interpretation of "data" under the PDPA is, however, not the widest among the referenced jurisdictions. New Zealand and Canada have read a wider meaning of "data" into the Privacy Act 1993 ("NZPA") and PIPEDA respectively. Even though the NZPA and PIPEDA do not define "information", the analogue to "data" under the PDPA, "information" has been judicially defined in both Canada and New Zealand as including unrecorded information.[92] As noted by the Law Commission of New Zealand, "unrecorded matter

87 Cap 486.
88 Personal Data (Privacy) Ordinance 1995 (Cap 486) (Hong Kong) s 2.
89 Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data, WP 136* (20 June 2007) at p 7.
90 Privacy Act 1988 (Act No 119 of 1988) (Cth) s 6.
91 *Vice-Chancellor Macquarie University v FM* [2005] NSWCA 192 at [28].
92 Paul Roth, *Privacy Law and Practice* (Wellington: LexisNexis, Privacy Act 1993, Looseleaf, 2007) PVA 2.12 at p 152.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

held in a person's mind can be 'information'".[93] That unrecorded information can constitute personal data is also affirmed by the Canadian Federal Court, which held that the lack of recording only affects the issue of collection of personal data but not the fact that the information is personal data.[94]

67 This wider reading of "data" is not without its problems. As acknowledged by the Law Commission of New Zealand in its review of the NZPA,[95] "evidential problems may arise"[96] especially over the existence of the information concerned and whether its content can be "known, accepted or understood" with any precision.[97] The Law Commission of New Zealand has also noted that "the inclusion of information that exists only in a person's mind appears to set the NZPA apart from most overseas privacy legislation".[98]

(c) "Data" as recorded information under the PDPA

68 Notwithstanding the broader scope of "data" found in the NZPA and PIPEDA which would make it ostensibly more consistent with the broad and expansive reading of personal data under the PDPA, it is submitted that "data" under the PDPA should apply only to recorded information. Besides the difficulties associated with admitting unrecorded information as noted in the previous paragraph, adopting a reading of "data" that requires recorded information is also more consistent with the majority of jurisdictions and in line with global trends. New Zealand and Canada are the only two referenced jurisdictions that admit unrecorded information. Hence a reading of "data" that requires recorded information should be adopted under the PDPA as it promotes the purpose of putting Singapore on par with major economies that have data protection laws so as to facilitate trans-boundary data transfer. It will also obviate evidentiary problems for administrators and organisations.

69 On the other hand, adopting a definition of "data" as including information that is recorded by any means and in any form is consistent with the technology-neutral nature of the PDPA. During the second reading of the Bill, the Minister stated that "it is important to note that

93 Law Commission of New Zealand, *Review of the Privacy Act 1997 – Review of the Law of Privacy Stage 4* (Issues Paper 17, March 2010) at para 3.6.
94 *Morgan v Alta Flights Inc* (2006) FCA 121 at [20].
95 Law Commission of New Zealand, *Review of the Privacy Act 1997 – Review of the Law of Privacy Stage 4* (Issues Paper 17, March 2010) at para 3.6.
96 Law Commission of New Zealand, *Review of the Privacy Act 1997 – Review of the Law of Privacy Stage 4* (Issues Paper 17, March 2010) at para 3.10.
97 *A and A v G* (13 July 1999) Complaints Review Tribunal 18/99 at para 16.
98 Law Commission of New Zealand, *Review of the Privacy Act 1997 – Review of the Law of Privacy Stage 4* (Issues Paper 17, March 2010) at para 3.6.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

the Bill adopts a principle-based and technology-neutral approach and it does not require that organisations put in place costly systems to manage and safeguard personal data".[99] That "data" under the PDPA is indifferent to the means and form in which information is recorded and kept means that it can easily lend itself to new technological developments. Furthermore, technological neutrality also promotes the interests of private organisations as compliance costs will likely be better managed when private organisations can elect the most cost effective technological solution for their personal data needs. Needless to say, it will also meet the expectations of individuals seeking greater protection, since more and more of their personal data is being recorded and stored in the electronic/digital format.

(2) "[W]hether true or not"

70 As observed earlier in this article, the qualifier of "whether true or not" found in the definition of personal data under the PDPA, was probably inspired by Australia's Privacy Act[100] ("AUPA"). The AUPA also has this qualifier worded in the exact same way.[101] As advised by the PDPC, the operation of this qualifier means that personal data under the PDPA "does not depend on whether the data is true or false".[102] In other words, the veracity of information is irrelevant when considering whether certain "data" is personal data under the PDPA. Explicit in the PDPC's advisory is therefore the view that false information identifying an individual could still be considered personal data.

(a) False information

71 While not specifically mentioned in their respective data protection legislations, the view that false information could constitute personal data nevertheless appears to be shared by the other referenced jurisdictions. As noted by the Article 29 Working Party in WP136, "[f]or information to be 'personal data', it is not necessary that it be true or proven".[103] In Canada, it also appears that false information could be considered personal data as the Canadian judiciary allows the filing of data protection complaints based on false information that identifies an individual.[104] In its review of the NZPA, the New Zealand Law

99 *Singapore Parliamentary Debates, Official Report* (15 October 2012) "Personal Data Protection Bill" vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Communications and Information).

100 Privacy Act 1988 (Act No 119 of 1988) (Cth).

101 Privacy Act 1988 (Act No 119 of 1988) (Cth) s 6.

102 Personal Data Protection Commission, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (24 September 2013) at para 5.7.

103 Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data, WP 136* (20 June 2007) at p 6.

104 *Lawson v Accusearch Inc* 2007 FC 125 at [9].

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

Commission also stated that, "with regard to false information, it seems clear that this is covered by the Privacy Act".[105]

72 Although the UK and Hong Kong are silent on this issue, they are probably amenable to false information being considered as personal data. As noted by the New Zealand Law Commission, "if false information did not fall within the coverage of 'personal information', principle 7 (which concerns correction of inaccurate information) would be nonsensical".[106] The authors find this argument to be persuasive. Hence, on that analysis, given that the UK and Hong Kong's data protection legislation both provide for the correction of inaccurate information under their respective data protection legislation, it logically follows that they would also consider false information as personal data. This logical extrapolation would similarly apply to the PDPA given that the correction of inaccurate personal data is also provided for under s 22 of the Act.

(b) Expressions of opinion

73 Besides false information, expressions of opinion could possibly also constitute personal data through the qualifier of "whether true or not". As noted, expressions of opinion are typically subjective in nature and it is not uncommon for expressions of opinion to be factually inaccurate to some extent. The admission of expressions of opinion would thus often require the use of this qualifier. Subjective types of information can include an opinion of facets of a person (*ie*, profiling) based on the evaluation of that individual's character, habits, preferences and proclivities through the assessment of his or her behaviour. There is a level of subjectivity inherent in such determinations that support opinion as personal data. This approach is not controversial or new. For example, the AUPA refers to "personal data" as "information or an opinion (including information or an opinion forming part of a database)".[107]

74 However, unlike the Australian example, the PDPA does not clearly or specifically include opinion as a form of personal data, notwithstanding the possibility of utilising the qualifier of "whether true or not" to include expressions of opinion as personal data. On the one hand, it would appear from the examination of the PDPA and the PDPC guidelines[108] that expressions of opinion cannot be personal data under

105 Law Commission of New Zealand, *Review of the Privacy Act 1997 – Review of the Law of Privacy Stage 4* (Issues Paper 17, March 2010) at para 3.6.

106 Law Commission of New Zealand, *Review of the Privacy Act 1997 – Review of the Law of Privacy Stage 4* (Issues Paper 17, March 2010) at para 3.12.

107 Privacy Act 1988 (Act No 119 of 1988) (Cth) s 6(1).

108 Personal Data Protection Commission, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (24 September 2013).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

the PDPA. The term "opinion of expression" was specifically removed from the PDPA's adaptation of the DPA's definition of personal data. There is also no mention of expression of opinion under the PDPC guidelines.

75 However, the authors of this article take the view, based on the earlier reasons given, that expressions of opinion should be personal data. Given the principle that identifiability of individuals is the crux to information constituting personal data, expression of opinion should be personal data if it is recorded and can similarly identify an individual. Specifically, it may be illusory to maintain that there is a difference between opinion and fact in relation to personal data. Whether information that can identify an individual, for instance about his preference for certain clothing brands, came about from the individual himself or from an analysis of his spending patterns should be immaterial in the determination of personal data. Moreover, in some cases, it may be difficult to separate what is a fact or an opinion about an individual. Maintaining this difference thus risks creating a possible loophole that can be exploited. Opinions about an individual, such as his or her interests and hobbies, also form an important and increasingly larger proportion of personal information collected and used, especially for sales and marketing purposes (*eg*, for target advertising). Finally, it should be noted that the Act also has provisions that refer to opinions ("including a professional or an expert opinion") and information for an evaluative purpose, which deal with various facets of a person's character that go beyond objective facts.[109]

76 As such, accepting opinion into the equation will avoid all these problems while providing greater protection for the individual under the broad and expansive reading of the PDPA provisions. That all the referenced jurisdictions recognise the potential for expressions of opinion to be personal data should also persuade the PDPC to take the view that opinions could be admitted as personal data under the PDPA.

109 See s 22(6) of the Personal Data Protection Act 2012 (Act 26 of 2012) in relation to an organisation's right not to have its opinions about an individual corrected, and the Second to Sixth Scheds that exempt an organisation from seeking consent (for collection, use and disclosure) and from the requirements to provide access and correction, respectively. It is of interest to note that personal data for evaluative purposes is generally exempted, hence providing a measure of relief to organisations (*ie*, in favour of their interest) due to the inclusion of expressions of opinion into the meaning of personal data (which is in the interest of the data subject).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

(3) "[A]bout an individual"

77 Data about an individual is the "most basic requirement for data to constitute personal data".[110] It is a separate inquiry (and element) from identifiability of a person. However, despite its importance, guidance from the PDPC on what constitutes data about an individual remains relatively scant. Specifically, the PDPC states that: "Data about an individual includes any data that relates to the individual".[111]

78 As noted at an earlier part of this article, the PDPA departed from the UK's DPA in adopting the term "about" as opposed to "relate to". As a result, two different readings of "about" which differ in their scope is possible. Information "about" or that "relates to" an individual can be given an expansive or narrow meaning.

(a) Narrow view of "about an individual"

79 One view, supported by Australia and New Zealand, is that the PDPA construes data about an individual in a more restrictive manner as the use of "about" connotes a narrower scope of association compared to that of "relate to". In this regard, the Judiciary in New Zealand has stated that "[t]he fact that information may become relevant to someone does not necessarily convert it into information 'about' that person".[112] It has also been noted that "[t]he Australian definition [of "about"] … reduces the scope of 'relating to' because it requires the information itself to have the capacity to identify without reference to other information"[113] although as earlier noted in this article, there is now no such reduction of scope following the recent amendment of the AUPA.

(b) Broad view of "about an individual"

80 Alternatively, if one takes the view that the change to "about" from "relate to" is immaterial and that the two terms are synonymous, the PDPA could construe data about an individual in a much broader manner identical to that adopted by the EU. As explained in WP136, "[i]n general terms, information can be considered to 'relate' to an individual when it is about that individual".[114]

110 Personal Data Protection Commission, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (24 September 2013) at para 5.3.

111 Personal Data Protection Commission, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (24 September 2013) at para 5.4.

112 *CBN v McKenzie Associates* [2004] NZHRRT 48 at [39].

113 Mark Burdon & Paul Telford, "The Conceptual Basis of Personal Information in Australian Privacy Law" [2010] MurUEJL 1 at 13.

114 Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data, WP 136* (20 June 2007) at p 9.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

81 Specifically, the Article 29 Working Party considered that data could "relate" to an individual if any of the three elements, *viz*, a "content", "purpose" or "result" element is present.[115] The "content" element is present when the "information is given *about* a particular person, regardless of any purpose on the side of the data controller … or the impact of that information on the data subject"[116] [emphasis added]. The "purpose" element exists when the information is used or is likely to be used "with the *purpose* to evaluate, treat in a certain way or influence the status or behaviour of an individual"[117] [emphasis added]. Lastly, a "result" element is present when the use of the information "is likely to have an *impact* on a certain person's rights and interests"[118] [emphasis added]. These approaches are not exhaustive or mutually exclusive and they all cover both objective and subjective forms of information. For example, purpose-based assessment covers subjective information such as data collected in order to evaluate, influence or in any other manner affect a person. It can be said that purpose and result based assessments are more contextual in nature, which are just as important as raw objective content.[119] They are often intricately linked. This is also indirectly acknowledged in the definition itself that refers to a combination of information as constituting personal data.

(c) UK's privacy-based view of "about an individual"

82 The UK, however, adopted a narrower but privacy-based view of "relate to" even though the DPA was required to be in line with the EU Data Protection Directive. Following *Durant*, a 2003 English Court of Appeal decision, the UK appears to have taken a narrower view of the meaning of information that "relates to" a person. Specifically, Auld LJ in *Durant* held that there are two notions in which information "relates to" an individual and stated that:[120]

> *The first is whether the information is biographical in a significant sense*, that is, going beyond the recording of the putative data subject's

115 Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data, WP 136* (20 June 2007) at p 10.

116 Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data, WP 136* (20 June 2007) at p 10.

117 Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data, WP 136* (20 June 2007) at p 10.

118 Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data, WP 136* (20 June 2007) at p 11.

119 "Focusing on the actual content of a particular data entry improperly negates the importance of contextual inferences". Scott Rempell, "Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: *Durant v Financial Services Authority* as a Paradigm of Data Protection Nuances and Emerging Dilemmas" (2006) 18 Fla J Int'l L 807 at 831, criticising the court's narrow construction of what constitutes personal data in *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

120 *Durant v Financial Services Authority* [2003] EWCA Civ 1746 at [28].

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

> involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised. *The second is one of focus.* The information should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest, for example, as in this case, an investigation into some other person's or body's conduct that he may have instigated. *In short, it is information that affects his privacy, whether in his personal or family life, business or professional capacity.* [emphasis added]

This privacy-based view of "relate to" means that personal data under the DPA will also be construed in a more limited manner when compared to WP136's articulation of "relate to" although this view will still be broader than the view taken by Australia and New Zealand. Under *Durant*, biographically insignificant data would not be personal data, even though this would still be personal data under WP136. On a separate but related note, it is interesting and apposite to note that this privacy-based view is very similar to what has been adopted by the Canadian judiciary[121] even though the PIPEDA uses the term "about an identifiable individual" as opposed to "relate to".

83 Efforts to reconcile these two approaches to "relate to" have been unsuccessful thus far. Even though the UK Information Commissioner maintains that its technical guidance on determining what is personal data ("technical guidance") "is consistent with [both] the approach taken by the [Article 29] Working Party [and *Durant*]",[122] it is hard to see how the technical guidance reconciles the two conflicting approaches. To try to align the technical guidance with both *Durant* and WP136, the UK Information Commissioner added the above two notions of "relate to" under *Durant* to the three elements found in WP136 to the technical guidance. However, this only ensured that the technical guidance is in line with WP136 but not *Durant*. Biographically insignificant data still cannot be personal data under *Durant* but the technical guidance has no such prohibition.

84 A tension hence emerged between the technical guidance of the UK Information Commissioner, that supports WP136, and *Durant*, and this tension has not gone unnoticed. In *Mr Tony Harcup v The Information Commissioner and Yorkshire Forward*[123] ("*Harcup*"), the UK

121 *Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board)* 2006 FCA 157.

122 United Kingdom, Information Commissioner's Office, *Data Protection Technical Guidance – Determining What is Personal Data* (12 December 2012) at p 3.

123 EA/2007/0058.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

Informational Tribunal[124] remarked that "[they] have difficulty in reconciling the approach in the Guidance [of the Information Commissioner] with that in *Durant*".[125] The Article 29 Working Party also noted, in a separate opinion,[126] that:[127]

> … in so far as such an interpretation [as a result of the decision in *Durant*] restricts the definition of personal data of the Directive, this may compromise the extent to which the Jersey legislation [which is *in pari materia* with the DPA] protects Personal Data.

85 However, a recent Court of Appeal decision appears to reduce the significance and influence of the *Durant* case, albeit without overruling that decision. In *Edem v The Information Commissioner & Financial Services Authority*[128] ("*Edem*"), the Court of Appeal did not overturn *Durant* with its "biographical significance" or "focus" analysis of the "relate to" requirement; however, the court distinguished *Durant* and seemed to relegate those narrow grounds to "borderline cases".[129] In *Edem* itself, which was not such a borderline case, the name itself, which was the subject matter of the dispute, constituted personal data. The only exception would be the case where a name is so common that it will not be able to identify an individual.[130] Thus, the court seems to signal that the tests in *Durant* are not strict and do not have to be universally applied to the point of absurdity in some cases following *Durant*. The effects of this new twist on future cases and whether the

124 The Information Tribunal heard appeals from notices issued by the Information Commissioner under the Data Protection Act 1998 (c 29) (UK) and other Acts. In 2010, the Information Tribunal was absorbed into the General Regulatory Chamber ("GRC") and now forms part of the First-tier Tribunal (Information Rights) of the GRC.

125 *Mr Tony Harcup v The Information Commissioner and Yorkshire Forward* EA/2007/0058 at [20].

126 Article 29 Data Protection Working Party, *Opinion 8/2007 on the Level of Protection of Personal Data in Jersey, WP 141* (9 October 2007).

127 Article 29 Data Protection Working Party, *Opinion 8/2007 on the Level of Protection of Personal Data in Jersey, WP 141* (9 October 2007) at p 4.

128 [2014] EWCA Civ 92.

129 The Court of Appeal in *Edem v The Information Commissioner & Financial Services Authority* [2014] EWCA Civ 92 ("*Edem*") referred to the opinion of Buxton LJ (in *Durant v Financial Services Authority* [2003] EWCA Civ 1746 at [79]) that "[t]he notions … will, with respect, provide a clear guide in borderline cases". See *Edem* at [15]. Thus, the significance and reach of *Durant* is confined to similar types of "borderline cases", although what constitutes a borderline case is likely to be a fresh issue to be determined.

130 This use of a clear link or obvious reference to the person in question whose identity is the subject of the dispute over personal data was provided for in the Information Commissioner's Technical Guidance and referred to with approval by the court in *Edem v The Information Commissioner & Financial Services Authority* [2014] EWCA Civ 92 at [21]. The court's approach has its own problems by conflating the separate requirements of "about"/"relate to" and the identification elements (although they can overlap to some extent).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

Durant anomaly will be confined to the facts of that (and similar) cases remains to be seen.

(d) Adopting the broad view of "about an individual"

86 From the above, it is clear that the PDPA can adopt one of the three above-mentioned views on what "about an individual" should mean under the Act. Even though each of the views has some merits, the authors endorse the broad view of "about an individual".

87 The view that "about" is narrower than "relate to", adopted by Australia and New Zealand, is arguably persuasive as the PDPA also uses "about" and not "relate to". However, that the PDPC in its guidance[131] made it clear that the term "about" is synonymous with "relate to" means that this view is probably misconstrued.

88 The UK privacy-based way of reading "relate to" is also arguably persuasive as the personal definition provision in both the PDPA and DPA share an almost identical structure. However, this view is likely to be untenable. As noted earlier in this article, the right of privacy is not recognised in Singapore and given that the PDPA "does not seek to change any right or obligation conferred by or imposed under the common law",[132] a privacy-based view of data protection similar to the UK should not apply here. Moreover, as noted, this reading of the phrase has its own problems, which the Singapore courts should be cautious not to follow.

89 That the PDPC's guidance[133] equates the term "about" with "relate to" means that the EU's broad view, which is based on "relate to", is persuasive. Furthermore, the PDPA's adoption of the EU's broad view on "relate to" will also likely provide useful guidance for local jurisprudence on the issue as it will also allow the Singapore courts to use the non-privacy based tri-element framework that consists of "content", "purpose" and "result" as outlined in WP136. Besides, this is also the only view that supports a broad and expansive reading of personal data as the other two views invariably narrow the scope of personal data by having a more limited understanding of what constitutes "about an individual" under the PDPA. If this approach is taken, it will also be consistent with accepting that expressions of

131 Personal Data Protection Commission, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (24 September 2013) at para 5.3.

132 *Singapore Parliamentary Debates, Official Report* (15 October 2012) "Personal Data Protection Bill" vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Communications and Information).

133 Personal Data Protection Commission, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (24 September 2013) at para 5.3.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

opinion can also constitute personal data, since it has some relation with the "purpose" element.

90 In fact, it can be said that the whole purpose requirement and the objective of greater individual control over his or her personal information supports the argument that that information should be relevant or significant in some sense (*ie*, have some value, monetary or otherwise, directly or indirectly). This is also consistent with the focus on the need of organisations for such information (which often goes beyond biographical data alone) and the time-based requirement for the management and storage of such information. In Singapore, as the PDPA is not based on the notion of privacy at all, the UK position in *Durant* is unpersuasive and should not be followed. Instead, the more popular and more generous interpretation of this requirement should be followed. The difference between "about" and "relate to" is also irrelevant.

(4) "[A]n individual who can be identified"

91 Identifiability of the individual is another substantial element in the definition of personal data under the PDPA. It is a prerequisite for an individual to be identifiable before the "data" in question becomes personal data that can enjoy the protection accorded under the Act. While the previous elements of "data", "whether true or not" and (to a lesser extent) "about an individual" are mainly focused on the informational aspect of personal data, the identifiability element of "an individual who can be identified"[134] is focused mainly on the data subject, that is the individual who is or who can be identified by the "data" at hand, as well as any other information that is accessible to the organisation in question relating to the person of interest.

92 The PDPC has provided more guidance on this matter. The PDPC has advised that "[a]n individual can be identified if that individual can be singled out from other individuals by an organisation based on one or more characteristics of the data or other pieces of information".[135] Further, identification of an individual can either be conducted "directly" or "indirectly". Where "an individual may be identified from a piece or set of personal data", such an individual is "directly" identified.[136] However, if "an individual [is] … identified based on certain data and other information to which the organisation has or

134 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).

135 Personal Data Protection Commission, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (24 September 2013) at para 5.9.

136 Personal Data Protection Commission, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (24 September 2013) at para 5.10.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

is likely to have access" then this individual is "indirectly" identified.[137] However, notwithstanding the above guidance provided by the PDPC, four areas of uncertainty remain.

(a) Burden of proof in identification

93 First, uncertainty remains over the burden of proof required in the identification of individuals as the PDPC has, thus far, been silent on this issue. Does this mean that identification is to be assessed on a balance of probabilities or, as aptly put by the New Zealand Law Commission which was considering the issue, "is it reasonably practicable, rather than merely theoretically possible, to identify the individual?"[138]

94 The other referenced jurisdictions have taken differing views on this issue. For example, Canada takes the view that an individual is identifiable when there is a "serious possibility"[139] that an individual could be identified through the use of that information, alone or in combination with other available information. In contrast, Australia and Hong Kong have provided in their legislation, the standard of "reasonableness", which means "reasonably ascertainable"[140] or "reasonably identifiable"[141] in the case of the former and "reasonably practicable"[142] in the latter case. Meanwhile, the EU position is that the identifiability of an individual is assessed by looking at all the means "likely reasonably"[143] used by the identifying party. As for the UK, the UK Information Commissioner has stated that:[144]

> [T]he fact that there is a very slight hypothetical possibility that someone might be able to reconstruct the data in such a way that the data subject is identified is not sufficient to make the individual identifiable … [and that the] person processing the data must consider all the factors at stake.

137 Personal Data Protection Commission, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (24 September 2013) at para 5.11.

138 Law Commission of New Zealand, *Review of the Privacy Act 1997 – Review of the Law of Privacy Stage 4* (Issues Paper 17 March 2010) at para 3.22.

139 *Gordon v Canada (Health)* 2008 FC 258 at [34].

140 Privacy Act 1988 (Act No 119 of 1988) (Cth) s 6.

141 Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Act No 197 of 2012) (Cth) s 6.

142 Personal Data (Privacy) Ordinance 1995 (Cap 486) (Hong Kong) s 2(1).

143 Directive 95/46/EC of the European Parliament and of the Council (24 October 1995) (protection of individuals with regard to the processing of personal data and on the free movement of such data) at Recital 26.

144 United Kingdom, Information Commissioner's Office, *Data Protection Technical Guidance – Determining What is Personal Data* (21 August 2007) at p 8.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

Further, the UK Information Commissioner also noted that:[145]

> When considering identifiability it should be assumed that you are not looking just at the means reasonably likely to be used by the ordinary man in the street, but also the means that are likely to be used by a determined person with a particular reason to want to identify individuals.

95 Although it thus remains uncertain as to which view the PDPA prescribes, it is submitted that the UK's views on this issue ought to be persuasive. The DPA shares the exact wording of "who can be identified" with the PDPA. Furthermore, setting the burden of proof for identifiability at a higher level than theoretical possibility as the UK has done by discounting "very slight hypothetical possibilit[ies]" and "consider[ing] all the factors at stake", is also aligned with Parliament's intention to keep compliance manageable and reasonable.

(b) "[L]ikely to have access"

96 Secondly, the meaning of "likely" as employed by "indirect" identification under the PDPA remains unclear. While "direct" identification appears to be straightforward and involves determining whether all the "data" at hand identifies an individual, "indirect" identification is less so.

97 Under the PDPA, individuals can be "indirectly" identified in two ways. First, an individual is identified "indirectly" if the identifying party is "in the possession of ['other information']"[146] and that "other information" when combined with the data at hand identifies an individual. This mode of "indirect" identification is not unlike "direct" identification. The identification of an individual is through the combination of "other information" as held by the identifying party with the data at hand; hence, the only difference that this form of "indirect" identification has with "direct" information is the additional determination of the possession of "other information" by the identifying party.

98 Alternatively, an individual is also "indirectly" identified if the identifying party is "likely to come into the possession of ['other information']"[147] and that the "other information" when combined with the data at hand identifies an individual. In this situation, however, there is the additional requirement to determine the content of the "other information" and the "likely" possession of such "other information"

145 United Kingdom, Information Commissioner's Office, *Data Protection Technical Guidance – Determining What is Personal Data* (21 August 2007) at p 9.

146 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).

147 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

by the identifying party. The degree of identifiability in "indirect" identification in this circumstance is more uncertain. The assessment involves determining what the acceptable sources of such additional information are and the ease and ability of the identifying party to avail itself of such information.

99 The PDPC has thus far not provided any guidance on what "likely" entails under the PDPA. There has also been no pronouncement on this issue from the UK, the only referenced jurisdiction that shares this sub-provision with the PDPA. Notwithstanding the above, it is submitted that "likely" could either connote "reasonably practicable", "probable" (that is more likely than not on a balance of probabilities) or "theoretically possible". In the authors' view, "likely" as "probable" should be adopted.

100 Adopting a "reasonably practicable" view is arguably undesirable. *Prima facie*, reading reasonable practicability into "likely" appears to be at odds with the plain meaning of "likely". The plain meaning of "likely" is descriptive and suggests a state of possibility but reasonable practicability is necessarily prescriptive as the identifying party would be obliged to possess "other information" when it is reasonably practicable. Further, adopting the view of "likely" as reasonably practicable also appears to be duplicitous, given that the means of identification is considered reasonably practicable.

101 Reading "theoretically possible" into "likely" should also be avoided. Notwithstanding the fact that "likely" on its face indicates a better chance of an event occurring than what is possible, having a meaning of possible possession as opposed to probable possession of "other information" is likely to make compliance overly onerous as it would unduly expand the scope of applicable "other information".

102 Thus, adopting the view of "likely" as being "probable", that is, more likely than not on a balance of probabilities, better conforms to the plain meaning of "likely" and is consistent with Parliament's intention to prevent compliance costs from becoming too onerous on private organisations.

103 For completeness, it should be noted that the addition of "access" serves to create yet another safeguard against an overly expansive definition under the PDPA as it is submitted that "data" must be accessible to an organisation before it can be considered to be personal data. Accessibility in this context refers to the ability of an organisation to obtain such "other data" that can used with the "data" at hand to constitute personal data. Such "other data" can include "publicly available information" (an issue that will be further considered below) as well as existing information that belongs to the organisation or

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

information held by its affiliates and partners that the organisation has the ability and/or the right to obtain if required. Hence, where information is not "accessible", this will have an impact on both the content and "likely" element of the "other data". The content of the "other data" will in this case be undeterminable while the inability to obtain such "other data" means that it cannot be "likely".

(c) Personal data in indirect identification

104 Lastly, uncertainty also remains over whether data used to "indirectly" identify individuals are by themselves personal data. As recalled earlier, "indirect" identification occurs when the identifying party makes use of the "data" at hand together with "other information" to identify an individual. Specifically, there is the issue of whether a piece of data that is used in conjunction with personal data to identify an individual will be personal data. Even though the combined information is undoubtedly personal data, it is unclear if such data by itself would be considered personal data.

105 No guidance on this issue has yet emerged from the PDPC. However, helpfully, guidance can be obtained from the UK which, in the DPA,[148] has an *in pari materia* sub-provision with the PDPA[149] on "indirect" identification. In *Common Services Agency for the Scottish Health v the Scottish Information Commissioner*[150] ("*Common Services*"), Lord Hope, with the agreement of Lord Hoffman, Lord Mance and Lord Rodger, in the House of Lords gave the following holding:[151]

> The relevant part of the definition … directs attention to 'those data', … and to 'other information' which is or may come to be in the possession of the data controller. *'Those data' will be 'personal data' if, taken together with the 'other information', they enable a living individual to whom the data relate to be identified. The formula which this part of the definition uses indicates that each of these two components must have a contribution to make to the result.* Clearly, if the 'other information' is incapable of adding anything … [t]he 'other information' will have no part to play in the identification. The same result would seem to follow if 'those data' have been put into a form from which the individual or individuals to whom they relate cannot be identified at all, even with the assistance of the other information from which they were derived. In that situation a person who has access to both sets of information will find nothing in 'those data' that will enable him to make the identification. It will be the other

148 Data Protection Act 1998 (c 29) (UK) s 1(1)(b).

149 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).

150 [2008] UKHL 47.

151 *Common Services Agency for the Scottish Health v the Scottish Information Commissioner* [2008] UKHL 47 at [24].

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

> information only, and not anything in 'those data', that will lead him to this result. [emphasis added]

106 It thus appears from *Common Services* that in order for "data" or "other information" to constitute personal data when "indirectly" identifying individuals, both of these elements "must have a contribution to make" to the identification of the individual. This position is logical and the greater implication that stems from this conclusion is that it prevents an overly wide definition of personal data. To decide otherwise would open the floodgates for almost any data or information that is used in conjunction with personal data to be classified as personal data simply by association.

(d) The relationship between "likely to have access" and "publicly available" data

107 Another interesting issue has to do with the relationship between the phrase "information to which the organisation … is likely to have access" and "personal data that is publicly available", which appears under the Second to Fourth Scheds (and for which an exception from the requirement to obtain consent applies).[152]

108 It is to be noted that the phrase "the personal data is publicly available" appears under the above-mentioned Schedules, whereas "personal data" is defined in the body of the Act, under the interpretation provision.[153] If it is to have the same meaning in the exception as in the interpretation, then the logical conclusion is that *all* the information referred to – new, old and accessible – must be public for the exception to apply. If the understanding is that the *entire* set of data must be publicly available for the exception to apply (*ie*, rather than only that *component* that is publicly available), then it reasonably follows that publicly available data as a component of identifiable data (*ie*, a mix of private and public information) *can also* constitute personal data (as long as that set of data remains intact). That means that information within an organisation's reach or "access" can still include publicly available information, if that data in itself cannot identify an individual but can, combined with data at hand and other (non-public) accessible data, contribute to the identification of an individual.

109 Alternatively, it may be argued that any component data whatsoever, *even that* which in itself cannot identify an individual, falls under the exception. In such a case, a more complicated problem arises.

152 Paragraph 1(*c*) of Second Sched, para 1(*c*) of the Third Sched and para 1(*d*) of the Fourth Sched read with s 17 of the Personal Data Protection Act 2012 (Act 26 of 2012).

153 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

On the positive side, an organisation can exclude more "personal data" from the consent requirement for collection, use and disclosure on the basis that an integral link in the chain that forms identifiable information is exempted. On the other hand, the task of the organisation (as well as the complainant and investigator) is rendered that much more complicated as they would have to break down each component of data (according to its source), determine and exclude public information, and then determine whether the rest of the data not so excluded can still identify an individual.

110 The third possibility is that publicly available data does not constitute or does not fall under "other information" to which an organisation "is likely to have access", which will have wider implications than the exception to the consent requirement. The definition of "publicly available" data as it is defined under s 2 does not refer to the word "access" but rather to what is "public", which is not helpful.[154] However, if this approach is taken, then it does not make sense to have the exception for "publicly available" information under the said Schedules in the first place. Moreover, the ordinary meaning of accessible information has a wider meaning than public information.

111 In the authors' opinion, the first approach to reconciling the two types of information is the preferred and most logical approach. It is also a simpler solution to the issue and is consistent with their position on other non-public types of "other data" that "indirectly" identify an individual.

C. Excluded personal data

(1) Overview of exclusions

112 Even when a piece or collection of information constitutes personal data, an individual or organisation that would otherwise be obligated to observe the PDPA requirements can still find respite under one of the general exceptions under s 4 ("Application of Act"). For example, "individuals acting in a personal or domestic capacity", employees acting in the course of employment, data intermediaries, public agencies and organisations as well as specifically exempted entities under subsidiary legislation by the Minister. There are two other exclusions that shall be looked at in greater detail: information excluded

154 As it stands, the fact that it is defined as such can either mean that (a) accessible information means information other than that which is ordinarily publicly available or (b) it is wider than (but including) publicly available information (*eg*, information available to all organisations within an industry or that can easily be obtained (for free or at a cost) from another organisation (*eg*, a data depository like a job search database).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

due to time limitations and the exclusion of "business contact information".

113 In relation to the former, these include "personal data about an individual that is contained in a record that has been in existence for at least 100 years",[155] and "personal data about a deceased individual" who has been dead for longer than ten years.[156] Even in relation to personal data about a deceased individual who has been dead for ten years or fewer, the PDPA provides a more limited form of protection, that is, only the application of "provisions relating to the disclosure of personal data and section 24 (protection of personal data)".[157]

(2) Some observations on business contact information

114 While the first two categories of excluded personal data – that is personal data older than 100 years and about deceased individuals – are quite self-explanatory, some observations can be made on the exclusion of business contact information.[158] Specifically, the definition of business contact information under the PDPA states that:[159]

> 'business contact information' means an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes …

From this definition, three observations can be made.

115 First, while a list of the different kinds of personal data has been provided under the definition above, this is not a closed list and "other similar" types of personal data could also become business contact information. This concept of similarity has two implications. First, it is submitted that this concept of business contact information is an affirmation of the technology-neutral nature of the PDPA as it is the informational and purpose aspect of the data that determines whether or not it is business contact information.

116 Perhaps more importantly, this similarity also relates to the type of information that could fall within the business contact information exclusion; that is, only information that could be used to contact an individual could become business contact information. Hence, this means that not all information offered by an individual for a business

155 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(4)(*a*).
156 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(4)(*b*).
157 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(4)(*b*).
158 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(5).
159 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

purpose or "[not] solely for his personal purposes" will become business contact information even if provided voluntarily. For instance, the provision of a person's national registration identity card ("NRIC") number to sign up for a gym membership will not, under this view, be business contact information, as NRIC numbers cannot be used to contact a person.

117 While this view has not been specifically endorsed by the PDPC, some support for this view can be found from the PDPC's explanation of business contact information in the guidelines. For instance, the PDPC states that:

> The definition of business contact information is dependent on the purpose for which such contact information may be provided by an individual as it recognises that an individual may provide certain work-related *contact information* solely for personal purposes [emphasis added].

Moreover, by taking a more circumscribed view of what information could possibly become business contact information is also in line with the purpose of the PDPA which advocates a balance between the right of individuals to personal data protection against the need of organisations to collect, use and disclose personal data. Allowing a wide meaning of business contact information, that is, all information provided for business is business contact information, would, however, likely lead to exploitation by organisations at the expense of individuals.

118 Second, it would also appear that for personal data to be business contact information, the personal data concerned needs to be given by the individual or collected with the consent of the individual identified by the personal data. Hence, where personal data has not been provided by or collected with the consent of the individual identified by the personal data, it is submitted that such personal data would not be excluded on the basis of it being business contact information.

119 Third, it would appear that as long as personal data was "not provided by the individual *solely* for his personal purposes" [emphasis added], the personal data could be excluded as business contact information. This approach gives a rather expansive view of business contact information for, so long as personal data was provided with some business contact purpose in mind, regardless of how large or minor this factor was, the personal data would be excluded as business contact information.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

VI. Conclusion

120 As is evident from this article, the Singapore Parliament intends for the PDPA to provide a robust and nuanced data protection framework that serves to promote the rights of individuals to data protection, the needs of organisations for access to personal data and also Singapore's efforts to become an international data hub that is jurisprudentially aligned with major economies. While some tensions exist between these different policy aspirations, it would appear that a purposive view of the PDPA would mean according a broad and expansive reading to personal data especially given the general scheme of the Act.

121 Moreover, the PDPA also represents an ambitious effort by the Singapore government to create a data protection regime that best serves Singapore by, *inter alia*, incorporating the best and most suitable aspects of data protection regimes from the referenced foreign jurisdictions. However, as this article has shown, this is not without some difficulty and despite guidance from the PDPC, some uncertainties over the meaning of "personal data", which is central to the coverage of the data protection provisions, remain. These include the proper approach to ascertaining the *identifiability* of an individual, what it is *about* an individual that is protected, the admissibility of expressions of *opinion* and the requirement for data to be recorded. Nevertheless, it is almost certain that some, if not all, of these uncertainties will be addressed in due course and that the concept and ambit of personal data under the PDPA will stabilise over time even though new questions over the PDPA will likely also emerge in their place. In the meantime, it is hoped that this article has made some useful suggestions on the ambit of "personal data" that can provide guidance to the stakeholders in the interim, and it is also hoped that the proposals will be considered and adopted by the PDPC and the courts when they have the opportunity to make an advisory and a ruling on the matter respectively.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

Appendix

SPECIFIC EXAMPLES OF PERSONAL DATA UNDER THE PDPA

1 In deciding whether certain classes or types of information are personal data, it should be kept in mind that the general principle governing such determination is whether the information could by itself or with other information lead to the identification of an individual.

2 As noted earlier, while it is certainly personal data if the information "directly" identifies the individual, where the information cannot by itself lead to the identification of an individual, much will then depend on the context at hand. Specifically, the information will only be personal data if the information can lead to "indirect" identification. Where "indirect" identification is involved, it is also important to recall from the earlier part of this article, that the information will only be personal data if it contributes to the identification of the individual.

3 Lastly, notwithstanding the above determination, there is also the need to consider the purpose under which the information is provided, as personal data may otherwise be excluded as business contact information.

4 In the following sections of this article, we will attempt to look at three common types of information – IP addresses, phone numbers and e-mail addresses – to determine whether they constitute personal data in the context of the PDPA by applying the above analysis.

A. IP addresses

5 With regard to IP addresses, it appears that much will depend on the context under which the IP address is collected. Specifically as noted by the PDPC, "an IP address, or any other network identifier such as an IMEI number, may not be personal data when viewed in isolation, because it simply identifies a networked device".[160] Thus IP addresses will not be personal data if IP addresses are collected solely for diagnostics or for tracking activities and the organisation cannot identify an individual from the data collected or from that data and other information to which that the organisation has or is likely to have access.

160 Personal Data Protection Commission, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (24 September 2013) at para 8.1.

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

6 Further, it is clear from the above that IP addresses cannot be used for "direct" identification of individuals. Consequently, IP addresses will only be considered personal data if they lead to the "indirect" identification of individuals and only if the IP addresses concerned contribute to the identification. For example, in a situation where a fixed IP address is assigned to a specific user account with an Internet Service Provider ("ISP") that is registered to and used by a specific individual exclusively, the said IP address would be personal data from the perspective of the ISP.

7 Lastly, given that IP addresses are seldom provided with the knowledge and consent of individuals or for the purpose of business contact, it is unlikely that IP addresses will be excluded as business contact information.

B. Telephone numbers

8 Like IP addresses, whether phone numbers will be personal data will largely be determined by the surrounding context. Given that telephone numbers do not identify individuals directly but instead identify specific telephony devices in the case of landlines or SIM cards in the case of mobile networks, telephone numbers, similar to IP addresses, will only be used for "indirect" identification of individuals. It thus follows that telephone numbers will only be personal data if they lead to the "indirect" identification of individuals and only if the telephone numbers concerned contribute to the identification.

9 Unlike the case for IP addresses, "indirect" identification of individuals via telephone numbers is likely to be easier. Telephone numbers are often closely linked to an individual, whereas IP addresses are mostly assigned randomly by ISPs. This is especially true for mobile telephone numbers as they are more likely to be associated with a unique individual.

10 Lastly, telephone numbers are more likely to be excluded as business contact information given that telephone numbers are routinely exchanged among individuals for business purposes. This view is supported by the PDPA, which among other possible types of personal data, lists telephone numbers in its definition of business contact information.[161]

161 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.

C. E-mail addresses

11 Unlike IP addresses and telephone numbers, e-mail addresses can potentially be used to "directly" identify individuals. Specifically, where the e-mail address itself reflects information that can lead to the "direct" identification of individuals – such as a person's full name, NRIC number or other similar types of information – they can constitute personal data.

12 However, where the e-mail address does not reflect information that can lead to the "direct" identification of individuals, e-mail addresses will only be personal data if they lead to the "indirect" identification of individuals and only if the e-mail address concerned contributes to the identification.

13 Lastly, similar to telephone numbers, e-mail addresses are also more likely to be excluded as business contact information given that e-mail addresses are increasingly (if not routinely) exchanged among individuals for business purposes. This view is supported by the PDPA, which among other possible types of personal data, lists e-mail addresses in its definition of business contact information.[162]

---

162 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).

© 2014 Contributor(s) and Singapore Academy of Law.
No part of this document may be reproduced without permission from the copyright holders.