Faculty of Law

Friday, 27 April 2012

Ministry of Information, Communication and the Arts
Singapore
via e-mail: MICA_DP_Bill_Consultation@mica.gov.sg

Dear Sir/Madam,

Public Consultation on the Proposed Personal Data Protection Bill

I am pleased to submit comments as requested on the draft legislation circulated by MICA. By way of background, I am a Professor of Law at the National University of Singapore. My academic interest in this area stretches back some years and I am presently working on an academic article on data protection that I hope to publish soon after the Data Protection Law is adopted.

The following text is in the form of commentary on the legislation that I hope will be helpful in the drafting process.

If I can be of any further assistance, please do not hesitate to contact me.

Yours faithfully,

Simon Chesterman

National University of Singapore Faculty of Law, 469G Bukit Timah Road, Singapore 259776
Tel: +65-651 67342 · E-mail: chesterman@nus.edu.sg
Website: law.nus.edu.sg
Company Registration No: 200604346E

A. Personal Data

Personal data is defined in the *PDPA* as:

> 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 is likely to have access.[1]

"Individual" is in turn defined as a natural person, whether living or deceased.[2]

This definition is similar to that used in the Model Code, but no longer limited to data in electronic form or to data concerning a living individual.[3] The former had been excluded for reasons of practicality,[4] but both in principle and in recognition of the amount of personal data routinely collected — for example, in the form of lucky draw and other competitions — it made sense to include such personal data in the Act.[5]

The inclusion of the personal data of deceased persons is more interesting. The EU lacks such a "protection", which appears to be modelled on Canadian legislation.[6] Such a provision calls into question the reason for data protection in the first place. Is personal data a property interest to be protected? If so, why is the limit only for 10 years? Or is data protection linked to protection of individual rights that pass with the individual? There is a legitimate interest in preventing personal details of recently deceased persons being made public, or the health details of relatives being sold to one's insurance company, but it is not clear that

---

[1] *PDPA [draft]* 2012 (Sing.), s. 2.

[2] *ibid*., s. 2.

[3] Cf. Model Code, para. 2.

[4] As the NIAC Report observed, paper records range "from the systematic to the shambolic": NIAC Report, para. 8.19.

[5] MICA March 2012 Public Consultation, para. 2.9.

[6] Cf. *PIPEDA* 2000 (Canada), s. 7(3)(h)(ii) (disclosure without knowledge or consent is permitted, *inter alia*, "twenty years after the death of the individual whom the information is about").

addressing these potential harms is best done through general inclusion in a data protection law. Again, the legislation suggests that it is best understood not with reference to protection of individualised rights to privacy so much as an attempt to govern information flows more generally. (The legislation is also interesting for the "compromise" that was struck between those who supported coverage for 20 years and those who opposed coverage entirely — resolved by a Solomonic decision to cover the personal data of deceased persons for 10 years only.[7])

In recognition of the tension between the global nature of information flows and territorialised jurisdictions, the Act is limited to personal data that has a "Singapore link".[8] This is satisfied if either the personal data or the individual whom it concerns was located in Singapore at the time of collection,[9] or if the personal data however collected is used or disclosed in Singapore.[10]

The Act is prospective, meaning that organisations may continue to use personal data collected prior to its entry into force for the same purposes.[11] That implied consent can be withdrawn by subsequent action,[12] but another exception covers situations in which an individual has "otherwise indicated", before or after the legislation enters into force, that he or she does not consent to the use of the personal data.[13]

1. Publicly Available Data

Business contact information is largely excluded,[14] as are personal data collected by observation at a performance, sports meet or a similar event.[15] Data "available to the public

---

[7] *PDPA [draft]* 2012 (Sing.), s. 4(4)(b).

[8] *ibid*., s. 5(1).

[9] *ibid*., s. 5(2)(a).

[10] *ibid*., s. 5(2)(b)-(e).

[11] *ibid*., s. 21.

[12] *ibid*., s. 21(1).

[13] *ibid*., s. 21(2).

[14] *ibid*., s. 4(5).

from a prescribed source" are also excluded — though what constitutes a prescribed source is not defined and must await the adoption of regulations.[16]

The approach is consistent with the Model Code, which did not limit the collection or use of data that are "generally available to the public",[17] nor the disclosure of data that are "generally available to the public in that form".[18] This is inconsistent with the EU position, however, in which public availability does not limit the application of data protection principles.[19] Interestingly, Canada's legislation, which was deemed adequate for EU purposes, does not restrict collection, use, or disclosure of data that are "publicly available *and* … *specified by the regulations*".[20] The relevant regulations list five categories of information, broadly covering (a) telephone directories; (b) professional directories; (c) registries compiled by statutory bodies and to which public access is authorised by law; (d) law reports; (e) published material where the relevant information has been provided by the individual him or herself.[21] Singapore could adopt a similar approach to exemptions. A key question would then be whether the posting of data on social networking sites such as Facebook or on a blog constitutes "publishing" that information.[22]

---

[15] *ibid*., 3rd Sched., para. 1(d).

[16] *ibid*., 3rd Sched., para. 1(c); s. 63(1).

[17] Model Code, para. 4.3(d), 4.4(d), 4.5(d).

[18] *ibid*., para. 4.5(m).

[19] See, *e.g.*, Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Article 29 Data Protection Working Party, 654/06/EN WP119, 25 March 2006) available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp119_en.pdf>.

[20] *PIPEDA* 2000 (Canada), ss. 7(1)(c), 7(2)(c.1), 7(3)(h.1) (emphasis added).

[21] Regulations Specifying Publicly Available Information (Ottawa: Canada Gazette, P.C. 2000-1777, 13 December 2000) available at <http://www.gazette.gc.ca/archives/p2/2001/2001-01-03/html/sor-dors7-eng.html>.

[22] Cf. Online Data Collection and Privacy: Discussion Paper (London: MRS Market Research Standards Board, 2011) available at <http://www.mrs.org.uk/standards/downloads/2011-07-19_Online_data_collection_and_privacy.pdf>, 6 (stating that posts on Facebook constitute personal data within the meaning of the EU Directive).

2. Sensitive Personal Data

The *PDPA* does not distinguish between different forms of personal data. Without using the word, the EU Directive provides stronger protections for data regarded as "sensitive". The UK implementing legislation established a special category of "sensitive personal data". Both require a higher threshold of consent before such data may be processed.[23]

There are on-going debates over the appropriate definition of sensitive personal data.[24] Malaysia's *Personal Data Protection Act* 2010 defines sensitive personal data as including medical history, political opinions, religious beliefs, and the commission or alleged commission of any offence.[25] Notable differences from the EU approach include the exclusion of racial or ethnic origin and sex life.[26] Singapore's Model Code drew heavily on the Canadian precursor to the *Personal Information Protection and Electronic Documents Act* 2000 (*PIPEDA*), and merely provided that when determining the form of consent appropriate to the processing of data, the sensitivity of those data should be taken into account.[27] In general, express consent should be required when the data in question are sensitive.[28] "Sensitive" was not defined in the Model Code, but the explanatory notes used the examples of medical and financial records as data that are almost always regarded as sensitive.[29]

The decision not to create a category of sensitive personal data in the *PDPA* was justified in part by the novelty of the regime being implemented and the possibility of sector-

---

[23] EU Data Protection Directive, art. 8; *Data Protection Act* 1998 (UK), s. 2.

[24] Peter Carey, *Data Protection: A Practical Guide to UK and EU Law*, 3rd edn (Oxford: Oxford University Press, 2009), 83.

[25] *Personal Data Protection Act* 2010 (Malaysia), s. 4.

[26] EU Data Protection Directive, art. 8(1).

[27] Model Code, para. 4.3.3. Cf. *PIPEDA* 2000 (Canada), 1st Sched., para. 4.3.4; Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act (Article 29 Data Protection Working Party, 5109/00/EN WP39, 26 January 2001) available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp39en.pdf>, 3.

[28] Model Code, para. 4.3.6.

[29] *ibid*., para. 4.3.3, Implementation and Operational Guidelines.

specific frameworks to address particular concerns.[30] This would include, for example, the *Banking Act* and existing codes for medical professionals.[31]

3. Children's Data

Whereas it is arguable that sensitive personal data enjoy some measure of sector-specific protection, a significant gap exists in the protection of the personal data of children.

This is an area in which the United States actually provides greater protection than Europe. The EU Directive — like the *PDPA* — does not refer to children specifically, meaning that the protections in place are the same as for their parents. Two implicit assumptions are that parents are aware of their children's activities online and are in a position to help guide them in making appropriate decisions. Neither assumption withstands much scrutiny when compared to the actual online behaviour of children. Some jurisdictions within Europe have adopted codes of conduct intended to regulate the activity of marketing, but these are generally regarded as weak or ineffectual.[32] (The draft Regulation now under discussion in the EU would include a new article on the personal data of children.[33])

The United States, by contrast, adopted legislation in the form of the *Child Online Privacy Protection Act* (COPPA) 1998, which came into force in 2000. It applies to commercial Web sites and online services directed at children aged under 13 and other Web sites that have actual knowledge that children aged under 13 are sharing personal information.[34] COPPA provides, among other things, requirements for the privacy policies of such sites, the circumstances in which "verifiable parental consent" must be obtained, and limitations on the use of any data collected. Though it is still possible to collect data, many sites now prohibit users under 13 completely — most prominently Facebook.

---

[30] MICA March 2012 Public Consultation, para. 2.8.

[31] See Notice Paper No. 116 of 2010, Question No. 462 for Written Answer (Singapore: Parliament, 19 July 2011) available at <http://app.mica.gov.sg/Default.aspx?tabid=231>.

[32] Emmanuelle Bartolia, "Children's Data Protection vs Marketing Companies" (2009) 23 Int'l Rev. L. Computers & Tech. 35.

[33] Proposal for a General Data Protection Regulation, art. 8.

[34] *Children's Online Privacy Protection Act (COPPA)* 1998 (U.S.), §§1302-3.

It is not clear that reliance on parental intervention is realistic, nor does the U.S. experience suggest that the costs to business of restricting collection of children's data are prohibitive. Nevertheless, accounts of parents tolerating or assisting their children creating Facebook accounts despite being under 13 are indicative of the relaxed attitude towards children's data protection in Singapore,[35] periodically tempered by scandals of abuse.[36]

It is possible that this will be revisited in the future.[37] One approach would be to require verifiable parental consent for the collection of the personal data of children, based on the U.S. law. Such consent can be verified in the United States through the submission of a credit card number or email, though these may be easily obtained by an enterprising child.[38] Alternative means of verification include provision of a handphone number, perhaps with some confirmation being sent via SMS, though an increasing number of children have their own phones. The most effective means of bypassing the media dominated by children may in fact be via "snail mail" — a letter.

B. Entities Affected

The *PDPA* applies to "organisations", defined as meaning "any individual, company, association or body of persons, corporate or unincorporated".[39] It covers organisations that collect, use, or disclose data in Singapore whether or not those organisations have a physical presence in Singapore. The decentralisation of modern telecommunications frequently gives rise to jurisdictional barriers to enforcement, but treating such organisations differently from those in Singapore might adversely affect local businesses.[40] Individuals acting in a personal or

---

[35] Jamie EE Wen Wei and TEO Wan Gek, "Kids Getting Internet Savvy at a Younger Age", *Straits Times*, 14 June 2009.

[36] Elizabeth Soh, "Most Severe Court Case of Underage Sex; Growing Danger from Young Kids Going Online, Say Social Workers", *Straits Times*, 30 December 2010.

[37] MICA March 2012 Public Consultation, para. 2.88. The Minister has the power, for example, to make regulations concerning the application of the Act to minors: *PDPA [draft]* 2012 (Sing.), s. 63(2)(b).

[38] Bartolia, "Children's Data Protection vs Marketing Companies", at 39.

[39] *PDPA [draft]* 2012 (Sing.), s. 2.

[40] MICA March 2012 Public Consultation, para. 2.17-2.20.

domestic capacity, or as employees of an organisation, are excluded.[41] Public agencies are excluded entirely.[42]

1. Data Intermediaries

One area in which the EU's approach to data protection had come to be seen as unnecessary or unhelpful was the distinction made between data controllers and data processors. In the EU Directive, as well as implementing legislation such as Britain's *Data Protection Act* 1998, data controllers determine why and how personal data are processed; data processors act on behalf of controllers.[43] The distinction was intended to be the degree of autonomy that an entity exercises over the processing operations, but in practice this distinction can be difficult to ascertain.[44] It is also somewhat at odds with modern information technology practices, particularly as increasing amounts of data are stored "in the cloud" and content is user-generated.[45]

The *PDPA* introduces the new concept of a "data intermediary", which is "an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation".[46] It is not clear why the term "data intermediary" was used rather than "data processor", since it is defined in almost identical

---

[41] *PDPA [draft]* 2012 (Sing.), s. 4(1)(a)-(b).

[42] *ibid.*, s. 4(1)(c). The MICA consultation paper states that government data protection rules accord "similar levels of protection" to that in the *PDPA*, but as those rules are not public this is difficult to evaluate. MICA March 2012 Public Consultation, paras. 2.12-2.16. An indication of possible openness may be seen in the regulation of medical records, which significantly affects public hospitals: TAY Sun Kuie, "The Impact of Data Privacy Protection in Medical Practice in Singapore" (2003) 12(4) SGH Proceedings 201. In addition, various government agencies have been accredited with the "TrustSg" mark. See, *e.g.*, Inland Revenue Authority of Singapore, available at <http://www.iras.gov.sg> (displaying TrustSg mark).

[43] EU Data Protection Directive, art. 2; *Data Protection Act* 1998 (UK), s. 1(1).

[44] See Carey, *Data Protection*, 211-2; Opinion 1/2010 on the concepts of "controller" and "processor" (Article 29 Data Protection Working Party, 00264/10/EN WP169, 16 February 2010) available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf>.

[45] See, *e.g.*, Vadim Schick, "Data Privacy Concerns for U.S. Healthcare Enterprises' Overseas Ventures" (2011) 4(2) J. Health & Life Sci. L. 173.

[46] *PDPA [draft]* 2012 (Sing.), s. 2.

terms with "processing" including, *inter alia*, adaptation and alteration of data.[47] This is particularly puzzling since the concept of a "data intermediary" with a significantly reduced role has been mooted in the academic literature[48] and proposed by industry.[49] If the intention is to define this category with reference to the EU standard, it might have been more appropriate to use the EU term. Otherwise, a narrower definition might have been better.

Data intermediaries have very limited obligations under the *PDPA* with respect to personal data processed for another organisation pursuant to a written contract.[50] These obligations are limited to the protection of data "by making reasonable security arrangements".[51] The organisation that has contracted with the intermediary remains fully responsible under the Act in respect of data processed on its behalf.[52]

2. News Organisations

A potentially interesting category is the limited exemption granted to news organisations. Such an organisation is exempted from the requirement to obtain consent for the collection, use, or disclosure of personal data "solely for its news activity".[53] Though the category is defined by reference to the type of organisation and activities undertaken, the key element is likely to be the requirement that any organisation must be gazetted as such by the Minister.[54]

---

[47] Cf. *Data Protection Act* 1998 (UK), s. 1(1).

[48] David Satola and Henry L. Judy, "Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum" (2011) 37 Wm. Mitchell L. Rev. 1745 at 1766.

[49] Vodafone's Response to European Commission Communication COM(2010) 609 (18 February 2011) available at <http://www.vodafone.com/content/dam/vodafone/about/privacy/vodafone_response_com2010_609.pdf> .

[50] *PDPA [draft]* 2012 (Sing.), s. 4(2).

[51] *ibid*., s. 26.

[52] *ibid*., s. 4(3).

[53] *ibid*., 3rd Sched., para. 1(j); 4th Sched., para. 1(j); 5th Sched., para. 1(l).

[54] *ibid*., s. 2.

C. Rules on Collection, Use, and Disclosure

The basic obligations under *PDPA* are that collection, use, and disclosure of personal data are permissible only with the actual or deemed consent of the individual, or where required by law.[55] Actual consent is only possible if the individual has been informed as to the purpose for which the personal data is being collected, used, or disclosed.[56]

An organisation cannot require an individual's consent to wider disclosure than is required for supplying a given product or service.[57] There was significant consideration, however, as to whether consent may be deemed if an individual has failed to "opt-out" of a data collection scheme.[58] The Act now limits deemed consent to circumstances in which an individual voluntarily provides the personal data and it is reasonable that he or she *would* provide the data.[59]

It is arguable that the EU requirement of unambiguous consent requires an opt-in approach — that is, the default position should be that data will not be shared with third parties or used other than for the purposes for which it is given.[60] (This is also the position taken in the draft Regulation that may soon supplant the EU Directive.[61]) In any case, based on the past decade's experience with the Model Code and the — at best — partial success of the *Spam Control Act*, the decision to require an opt-in approach with very limited provision for deemed consent is appropriate. Consent, however given, can be withdrawn with reasonable notice.[62]

---

[55] *ibid*., s. 15.

[56] *ibid*., ss. 16(1)(a), 22.

[57] *ibid*., s. 16(2): "An organisation shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal data beyond what is reasonable to provide the product or service to that individual."

[58] See MICA March 2012 Public Consultation, paras. 2.49-2.50.

[59] *PDPA [draft]* 2012 (Sing.), s. 17.

[60] See generally Michael E. Staten and Fred H. Cate, "The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA" (2003) 52 Duke L.J. 745 at 749.

[61] Proposal for a General Data Protection Regulation.

[62] *PDPA [draft]* 2012 (Sing.), s. 18.

In complying with these obligations, organisations are required to develop policies for implementation, including a process to respond to complaints.[63] Organisations are also required to "consider", when meeting those obligations, "what a reasonable person would consider appropriate in the circumstances."[64] How an organisation would engage in such contemplation is unclear, but there is separate provision that the purposes for which personal data is collected, used, or disclosed must be purposes "that a reasonable person would consider appropriate in the circumstances".[65]

These reasonableness caveats may aid in addressing one of the most basic problems in data protection regimes, which is analogous to the problems confronting privacy laws: in theory consent can regulate the appropriate flow of personal data; in practice consent routinely fails to do so either because consumers do not understand the options or companies do not give them a meaningful choice.[66]

Another provision that highlights the focus on information flows rather than privacy-type rights concerns access to and correction of personal data. Organisations are obliged to "make a reasonable effort" to ensure that personal data are "accurate and complete", if those data are likely to be used "to make a decision that affects the individual" or shared with another organisation.[67] An individual may generally request access to personal data and request the correction to errors or omissions in personal data concerning him or her.[68]

All organisations are required to protect personal data in their custody or control by "making reasonable security arrangements" to prevent unauthorised access.[69] Where data have

---

[63] *ibid*., s. 14.

[64] *ibid*., s. 13(1).

[65] *ibid*., s. 20(a).

[66] See generally Lisa M. Austin, "Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA" (2006) 56 U. Toronto L.J. 181; Matthew S. Kirsch, "Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising" (2011) 18 Rich. J.L. & Tech. 2.

[67] *PDPA [draft]* 2012 (Sing.), s. 25.

[68] *ibid*., ss. 23-24.

[69] *ibid*., s. 26.

been used to make a decision directly affecting an individual, they must be kept for at least one year;[70] otherwise, when "it is reasonable to assume" that the purpose no longer requires retention and there is no business or legal requirement, personal data must be destroyed.[71] This potentially broad requirement to destroy personal data will likely be offset by the ability to argue that retention is reasonably necessary for on-going business purposes.

1. Exceptions to the Requirement for Consent

The *PDPA* allows for the collection, use, or disclosure of personal data without consent in specified circumstances, elaborated in the Third, Fourth, and Fifth Schedules[72] — which may be amended by the Minister by order published in the *Gazette*.[73] The three schedules run to some eight pages, but there is significant overlap. Collection, use, or disclosure is permitted, for example, where it is "clearly in the interests of the individual" and consent cannot be obtained in a timely way; in response to an emergency; necessary in the national interest, or for an investigation or legal proceedings; for the collection of a debt; for the provision of legal services; or otherwise authorised by law.[74]

A further exclusion is made for "evaluative purposes", including decisions related to employment, admission to educational institutions, and contractual and insurance matters.[75] Exemptions are also made for "news organisations" discussed earlier,[76] and where collection, use, or disclosure is solely for "artistic or literary purposes".[77] Personal data may not be collected, but it may be used or disclosed without consent for certain research purposes.[78] And

---

[70] *ibid*., s. 27(1).

[71] *ibid*., s 27(2).

[72] *ibid*., s. 19.

[73] *ibid*., s. 62(1).

[74] *ibid*., 3rd Sched., para. 1; 4th Sched., para. 1; 5th Sched., para. 1.

[75] *ibid*., s. 2.

[76] See *supra* notes 53-54.

[77] *PDPA [draft]* 2012 (Sing.), 3rd Sched., para. 1(i); 4th Sched., para. 1(i); 5th Sched., para. 1(k).

[78] *ibid*., 4th Sched., para. 1(m); 5th Sched., para. 1(t).

a general exclusion allows for disclosure — but not collection or use — to a public agency if necessary in the public interest.[79]

2. Transborder Transfers

The original draft of Singapore's Model Code included an eleventh principle, said to be "optional", that covered transborder transfers of data and was loosely based on Article 25 of the EU Directive.[80] In its place, the Code as adopted provided only that organisations transferring data to any third party should "take reasonable steps to ensure that the data ... will not be processed inconsistently" with the Code.[81]

The *PDPA* does not embrace the EU approach of making adequacy determinations as to jurisdictions to which personal data may be transferred, but it does go further than the Code in that it removes the implicit defence of reasonableness. The Act does this in a slightly unusual way by omitting to mention transborder transfers — or transfers of any kind — at all. Instead, it provides that an organisation continues to have the same obligations under the *PDPA* in respect of "personal data processed on its behalf by a data intermediary as if the personal data were processed by the organisation itself."[82]

The intention was to ensure "that personal data will always be accorded a similar level of protection even if transferred outside Singapore" and to encourage parties to "engage the parties to which they transfer data".[83] Nevertheless, it is far from clear that this gives the kind of guidance that would be helpful to organisations contemplating sharing data. It is also not clear what legal obligations would follow in the event of transfer (presumably with consent) to an entity that is not a data intermediary.

There is an argument for treating transborder transfers differently from domestic disclosure of data: in the latter case, the entity is clearly subject to the Act. In the case of a transborder transfer, the third party might not be meaningfully subject to the Act. Protection of

---

[79] *ibid*., 5th Sched., para. 1(i).

[80] NIAC Report, paras 8.12, 8.47-8.50.

[81] Model Code, s. 4.1.1.

[82] *PDPA [draft]* 2012 (Sing.), s. 4(3).

[83] MICA March 2012 Public Consultation, para. 2.90.

the personal data in such cases might take the form of explicit consent to the transfer, or contractual arrangements to provide for alternative protections.[84] The U.S. Safe Harbor principles, by which the Department of Commerce provides a streamlined means for organisations to comply with the EU Directive, might provide a model in this regard.[85] But in the absence of additional guidance there is considerable scope for uncertainty.

3. Data Breach Notification

The Act does not include a provision requiring organisations to notify customers in the event that personal data is compromised. In 2008, the Australian Law Reform Commission recommended creating a new obligation to notify the Privacy Commissioner and affected individuals when an unauthorised person acquires personal data and there is a real risk of serious harm.[86] Similar requirements are being debated in the United States, in the wake of Citigroup's revelation that personal data from 200,000 credit card holders was stolen by hackers.[87]

A blanket obligation to report every breach could be excessively onerous. A recent proposal by the White House would have limited the obligation to organisations that collect personal data of 10,000 people in any 12-month period.[88] The ALRC threshold of "real risk of serious harm" would clearly encompass possible identity theft, but limit the need to report on data breaches that do not include identifying information.

Additional questions include identifying where data resides and who should be obliged to make the report: the organisation that collected the information in the first place and has a relationship with the customer, or the service provider who stored the data? In the U.S., state

---

[84] Connolly, Asia-Pacific Region, 6. This appears to have been accepted with respect to Canada: Opinion 2/2001 on PIPEDA, 6.

[85] Safe Harbor Privacy Principles (Washington, DC: U.S. Department of Commerce, 2000) available at <http://export.gov/safeharbor/eu/eg_main_018475.asp>.

[86] For Your Information, Recommendation 51-1.

[87] Eric Dash, "Citi Data Theft Points Up a Nagging Problem", *N.Y. Times*, 9 June 2011.

[88] Elizabeth Montalbano, "White House Seeks National Data-Breach Notification Law", *InformationWeek*, 13 May 2011.

legislation generally puts the onus on the former.[89] To whom should such a report be made? Where serious harm might follow, the customer should be advised. But more generally it would be desirable to have the supervisory authority — the Data Protection Commission — informed. Taiwan recently proposed amendments to its Data Protection Act (not yet in force) that would include a modest data breach notification requirement for violations of the Act, though it has been criticised for not having a supervisory body.[90]

An alternative approach to data breach notification is not to make it a mandatory obligation but to consider any such notification to those who might be injured by data breach as a mitigating factor in enforcement proceedings. If this is the case, reference to data breach notifications should be included in penalty guidelines that are drafted for enforcement purposes.[91] This is useful both in ensuring fairness but also in order to telegraph to organisations that it is in their interest to notify customers of data breaches.

4. Do Not Call Register

The slightly odd fit of the Do Not Call register within the *PDPA* is suggested by having its own interpretive clause.[92] The obligations created are additional to those in the *Spam Control Act*, on the basis that whereas that Act puts conditions on the sending of unsolicited commercial messages sent in bulk, the Do Not Call register determines whether a specified message may be delivered to a specific telephone number. "Specified message" for this purpose is defined by reference to the content, presentation, or linked information. If, having regard to that information, "it would be concluded" that one of the purposes of the message is to advertise or otherwise offer to supply goods or services, an interest in land, or a business or investment opportunity.[93]

---

[89] Jacqueline May Tom, "A Simple Compromise: The Need for a Federal Data Breach Notification Law" (2010) 84 St. John's L. Rev. 1569.

[90] Shamma Iqbal, "Taiwan Introduces Enforceable Data Breach Notification Requirements", *Inside Privacy*, 9 March 2011.

[91] Cf. MICA March 2012 Public Consultation, para. 2.112.

[92] *PDPA [draft]* 2012 (Sing.), s. 40.

[93] *ibid.*, s. 41.

Such messages may not be sent to a Singapore telephone number that has been entered on the Do Not Call register, regardless of where the sender or recipient are in Singapore at the time the message is sent or received.[94] Unlike the rest of the *PDPA*, the Do Not Call provisions apply to a "person" who sends such messages, who is under an obligation to check the Do Not Call register every 30 days.[95] Failure to comply is an offence punishable with a fine of up to $10,000.[96]

D. Enforcement

The *PDPA* establishes a Data Protection Commission consisting of three to seven members appointed by the Minister.[97] Its mandate includes enforcing the Act but also promoting awareness, conducting research, and advising the Government on data protection generally.[98] Provision is made for the Commission to produce non-binding guidelines, which will likely play an important role in implementation of the Act.[99]

The basic model of enforcement is complaints-based rather than audit-based, or what is sometimes termed "fire-alarm" rather than "police-patrol" regulation.[100] Where the Commission is satisfied that an organisation is not complying with the Act, it may direct the organisation to stop collecting, using, or disclosing personal data; to destroy personal data; and/or to pay a financial penalty of up to $1 million.[101] This is separate from the offences created, which include wilfully collecting, using, or disclosing personal data in contravention of

---

[94] *ibid*., ss. 42, 47(1).

[95] *ibid*., s. 47(1).

[96] *ibid*., s. 47(2).

[97] *ibid*., s. 6.

[98] *ibid*., s. 7.

[99] *ibid*., s. 28.

[100] Cf. Mathew D. McCubbins and Thomas Schwartz, "Congressional Oversight Overlooked: Police Patrols versus Fire Alarms" (1984) 28 Am. J. Pol. Sci. 165 at 166-76.

[101] *PDPA [draft]* 2012 (Sing.), s. 31. Decisions of the Data Protection Commission may be appealed to a new Data Protection Appeal Panel, with further appeal possible to the High Court: *ibid*. ss. 38-39.

the Act; evading an individual's request for access to personal data; and obstructing or misleading the Commission.[102] Where no other penalty is provided for, the maximum penalty is a fine of up to $10,000 and up to three years in prison.[103] Fines and other moneys are to be paid into a Data Protection Fund, which can then be used for expenses associated with administering the Act as well as promoting data protection awareness.[104]

Britain's Information Commissioner has a similar power to issue "enforcement notices" — requiring a data controller to take (or to refrain from taking) specified actions if the Commissioner is satisfied that the controller has contravened the data protection principles.[105] Beginning in April 2010, if there is a serious contravention that is likely to cause "substantial damage or substantial distress", and the controller knew or ought to have known that there was a risk of such an outcome, the Commissioner has also been able to impose monetary penalties of up to £500,000.[106]

The *PDPA* also provides that an individual who suffers "loss or damage directly as a result" of a contravention of the Act may also bring a civil suit against the organisation responsible.[107]

Finally, the Act includes a slightly unusual provision that one might term an "anti-supremacy" clause, which states that insofar as the Act is "inconsistent with any provision of other written law, the provision of the other written law shall prevail."[108] Though it is a relatively minor point, this sets up a potentially interesting challenge to another part of the Act concerning the ability of a legal counsel of the body administering the Act to act on its behalf "[n]otwithstanding the provisions of any written law".[109]

---

[102] *ibid*., s. 35.

[103] *ibid*., s. 54.

[104] *ibid*., s. 10.

[105] *Data Protection Act* 1998 (UK), s. 40.

[106] *ibid*., s. 55A.

[107] *PDPA [draft]* 2012 (Sing.), s. 36(1).

[108] *ibid*., s. 4(7) (emphasis added).

[109] *ibid*., s. 11(4).

Such provisions are overshadowed by the extraordinary power given to the Minister to "repeal or amend any written law in force on the appointed day *which appears to him to be unnecessary* having regard to the provisions of this Act or to be inconsistent with any provision of this Act".[110] Any such repeal or amendment may be done within two years after the Act comes into force by order published in the *Gazette*. This extremely broad language echoes similar language in a dozen other acts,[111] but on its face appears to raise constitutional difficulties as the power to pass, amend, or repeal statutes is clearly vested in the Legislature.[112]

---

[110] *ibid*., s. 62(2) (emphasis added).

[111] See *Regulation of Imports and Exports Act* 1995 (Cap. 272A, 1996 Rev. Ed. Sing.), s. 44; *Rapid Transit Systems Act* 1995 (Cap. 263A, 2004 Rev. Ed. Sing.), s. 47; *Maritime and Port Authority of Singapore Act* 1996 (Cap. 170A, 1997 Rev. Ed. Sing.), s. 120; *Port of Singapore Authority (Dissolution) Act* 1997 (Sing.), s. 15; *Environmental Protection and Management Act* 1999 (Cap. 94A, 2002 Rev. Ed. Sing.), s. 78; *Info-communications Development Authority of Singapore Act* 1999 (Cap. 137A, 2000 Rev. Ed. Sing.), s. 30(3); *Singapore Land Authority Act 2001 (Chapter 301) — rev ed 2002* 2001 (Cap. 301, 2002 Rev. Ed. Sing.), s. 38; *Intellectual Property Office of Singapore Act (Chapter 140) 2001 — 2002* 2001 (Cap. 140, 2002 Rev. Ed. Sing.), s. 38; *Payment and Settlement Systems (Finality and Netting) Act* 2002 (Cap. 231, 2003 Rev. Ed. Sing.), s. 22; *Accountants Act* 2004 (Cap. 2, 2005 Rev. Ed. Sing.), s. 69; *Limited Liability Partnerships Act* 2005 (Cap. 163A, 2006 Rev. Ed. Sing.), s. 60(2). Cf. *Fire Safety Act* 1993 (Cap. 109A, 2000 Rev. Ed. Sing.), s. 62(4) (empowering the Minister to repeal or amend laws which appear to him to be "inconsistent" with any of the provisions of this Act).

[112] *Singapore Constitution*, art. 58.