



美国何威律师事务所驻北京代表处

HUNTON & WILLIAMS LLP  
BEIJING REPRESENTATIVE OFFICE  
517-520 SOUTH OFFICE TOWER  
BEIJING KERRY CENTRE  
NO. 1 GUANGHUA ROAD  
CHAOYANG DISTRICT  
BEIJING, PRC 100020

TEL 86•10• 5863•7500

FAX 86•10• 5863•7591

September 21, 2017

**To: Singapore Personal Data Protection Commission (the “PDPC”), at  
corporate@pdpc.gov.sg**

**Re: PDPC’s Public Consultation on Approaches to Managing Personal Data in the  
Digital Economy**

Ladies and Gentlemen,

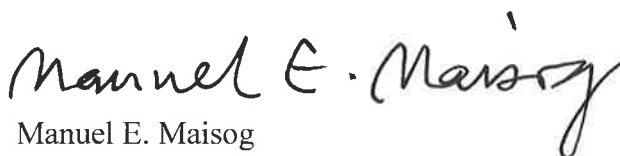
My name is Manuel Maisog and I am the Resident Partner and Chief Representative at the Beijing office of Hunton & Williams LLP, a U.S. law firm with a leading data privacy and cybersecurity practice. I am a member of that practice group. I am also a Principal of the Center for Information Policy Leadership, a policy think tank founded by and resident in our law firm’s offices, and for several years now have acted as a Delegate from the United States at meetings of the Data Privacy Subgroup of the Electronic Commerce Steering Group at the Asia-Pacific Economic Cooperation forum. I can be reached by e-mail at [bmaisog@hunton.com](mailto:bmaisog@hunton.com) and by telephone at 86-10-5863-7500.

I have comments on Part III (Mandatory Data Breach Notification) of the public consultation paper entitled *Public Consultation for Approaches to Managing Personal Data in the Digital Economy*, issued 27 July 2017 (the “**Public Consultation Paper**”). My colleagues at the Center for Information Policy Leadership will comment separately on Part II (Enhanced Framework for Collection, Use and Disclosure of Personal Data).

My comments reflect my own views only. They represent neither the views of Hunton & Williams LLP nor those of any of its clients. Also, they represent neither the views of the Center for Information Policy Leadership nor those of any of its member companies.

The comments are set forth on the pages following this cover page. I hope that they will prove useful. I am available to provide clarifications of any that may not be clearly stated.

Respectfully submitted,

  
Manuel E. Maisog



Cc: Lisa Sotto, Esq. (Hunton & Williams LLP)  
Brittany Bacon, Esq. (Hunton & Williams LLP)

Cc: Bojana Bellamy (Center for Information Policy Leadership)  
Markus Heyder (Center for Information Policy Leadership)

Singapore Personal Data Protection Commission, at corporate@pdpc.gov.sg  
September 21, 2017  
Page 2

## COMMENTS, AND AN INTRODUCTION THERETO

### *Introduction*

I should first provide an explanation of the perspective from which I have made the comments which follow.

An information security breach comes as an urgent and unpleasant surprise to a business enterprise. Certainly, they will already be pre-occupied with day-to-day (but nonetheless important) business tasks at the time. Very possibly, they will already also be pre-occupied with significant transactions at the time, such as a financing, acquisition or construction project. Once the information security breach arrives, much will be at stake. Not only will class action lawsuits from data subjects be in prospect, but the enterprise also now will face projects of litigation by business partners, reputational damage, loss of trust by consumers, and investigation and litigation by regulatory authorities. In addition, the duties and responsibilities involved in their normal business activities, and significant transactions (if any), means that management will in practice be able to dedicate nowhere near the appropriate level of their attention to the management of the incident. There will be a lot of stress, and anxiety.

In short, an information security breach is a crisis. But it is a crisis that has one very special aspect: In many instances, in the first several hours and even ranging into the first several days, weeks or even perhaps months, the affected enterprise *does not truly know what has actually happened to it*.

From the perspective of the affected enterprise itself, the first thing that really happens is not so much the information security breach itself, but the company's discovery that a data breach may have occurred. This is important to point out because it could be a long time, possibly even years, between the time when the information security breach incident actually occurred, and the time when the enterprise discovers it. As a result, at the moment when it discovers that a data breach may have occurred, the affected enterprise actually may not know or understand what has happened. During the early hours of its breach response effort, the enterprise may know only that *a* security breach incident *may have* occurred, and not very much more.

As you already know, because almost all information security breaches involve information that has been recorded or processed digitally, in the great majority of cases the breach itself necessarily takes the form of a digitally managed and digitally performed act. As such, evidence of the incident is left digitally. The enterprise cannot ascertain, simply by physically looking at its servers, such basic points of investigation as when the security incident took place; where the incident took place; what caused the incident; who caused the incident; whether any personal, sensitive or confidential information was involved and if so,

Singapore Personal Data Protection Commission, at [corporate@pdpc.gov.sg](mailto:corporate@pdpc.gov.sg)

September 21, 2017

Page 3

of what types and in what volumes; how many people were affected; and what the nature and likelihood of overall damage may be. A digital forensic investigation is often necessary to answer these questions. That investigation can take time and often cannot be completed in only a few hours. Very often, 24 or 72 hours will not be nearly enough.<sup>1</sup> Depending on how much time has passed since the information security breach took place, varying amounts of the evidence may have become corrupted and unreadable, been overwritten or otherwise somehow disappeared. The culprit may have taken care to cover his or her tracks, and left only limited evidence. It is possible that the affected enterprise over time will have to change its understanding of the facts of the case, or adopt new words to describe it. And in the early hours after the discovery of the breach incident, the affected enterprise may not even be able to turn its attention to commencing the investigation at all, because it may have to prioritize other even more urgent matters, such as containing and stopping a continuing leakage of further information, if it discovers a breach incident that is still in progress. This higher immediate priority of containing and stopping an ongoing breach incident may itself take many hours, or several days.

Technological advances are not necessarily going to make the digital forensic investigation easier or faster. Technological advances could instead add a complexity to the affected enterprise's information architecture that make the investigation process more challenging. Technological advances could also instead make it easier for the culprit to cover his or her tracks, and suppress or erase digital evidence of what he or she has done and how. In short, technological advances may actually make this process of the digital forensic investigation more difficult and longer.

The point is this. A hard and fast, and in particular an arbitrarily short, deadline for notification of a data breach incident is unrealistic. It is unrealistic because the whole point of a breach notification is to enable data subjects to understand what has happened and, on the basis of that understanding, to take action to protect their interests. But without an

---

<sup>1</sup> In the most recent major data security breach incident, Equifax discovered their data breach incident on July 29 of this year, and on August 2 contacted Mandiant to assist in conducting the forensic investigation. In other words, after 4 days, Equifax was only just commencing its forensic investigation. Equifax reports that Mandiant then analyzed available forensic data to identify unauthorized activity on the network "over several weeks." Equifax did not announce the security incident until September 7. *See* <https://www.equifaxsecurity2017.com/> and <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>.

This is a clear, practical, real-life example of how a 72-hour breach notification deadline not only would have been unrealistic, but also would have even pressured the affected enterprise to notify when its forensic investigation was only just getting started. A 72-hour breach notification deadline under such circumstances could be wholly counterproductive.

Singapore Personal Data Protection Commission, at corporate@pdpc.gov.sg

September 21, 2017

Page 4

accurate understanding of what has happened to it, the enterprise cannot make an accurate breach notification to the data subjects. And without an accurate breach notification, the data subjects cannot really know what they have to do to protect their interests. The enterprise may not even yet know, at the moment of the deadline, who it has to notify, or what information of theirs has been affected.

A hard and fast, or arbitrarily short, deadline therefore does not add a helpful or constructive element to a situation which the affected enterprise is already experiencing as a crisis. Instead, it adds a degree of unnecessary time pressure, stress, and potential liability. It may force the enterprise to describe the incident without yet knowing exactly what has taken place, and therefore expose it to accusations of having acted irresponsibly or with negligence. It fosters misinformation. It fosters uncontrolled misunderstandings. It simply creates additional risk, without mitigating risk.

For that reason, and as you will find in the comments that follow, I am recommending that if a mandatory breach notification framework is to be established in Singapore, it should allow the affected enterprise sufficient time and flexibility to allow it first to conduct its digital forensic investigation, and come to a clear and accurate understanding of what has really happened, before it is required to make any notification.

### *Comments*

My comments respond to Questions 5 through 8 of the Public Consultation Paper. As requested, where feasible I have identified the specific section of the Public Consultation Paper on which I am commenting, and explained the basis for my proposals.

***Question 5: What are your views on the proposed criteria for data breach notification to affected individuals and to PDPC? Specifically, what are your views on the proposed number of affected individuals (i.e., 500 or more) for a data breach to be considered of a significant scale to be notified to PDPC?***

My comment is in two parts.

1. One proposed criterion, in Section 6.2(a) of the Public Consultation Paper, would require affected enterprises to notify affected individuals and the PDPC of a data breach that poses “any risk” of impact or harm to the affected individuals. This goes too far. The term “any risk” includes even minor, immaterial and inconsequential risks. This would actually go further than the EU’s GDPR, which requires notification to the affected data subjects only when the breach is likely to result in a “high risk” to the rights and freedoms of data subjects.

The breach notification requirement would be more practical if it were to take a risk-based approach, under which the affected enterprise were given the opportunity to

Singapore Personal Data Protection Commission, at corporate@pdpc.gov.sg

September 21, 2017

Page 5

assess the likelihood of risk and the types of risk involved, and perform a notification requirement only where the risk of harm to a data subject appears likely and material. No notification requirement should apply in cases where the risk of harm to a data subject either does not appear likely, or does not appear to be material (or serious). The rationale for reporting only risks of material (or serious) harm is discussed below, in conjunction with my discussion of the criterion proposed in Section 6.2(b).

2. The other proposed criterion, in Section 6.2(b) of the Public Consultation Paper, would require data breach notification to the PDPC for all breaches which involve a minimum number of affected individuals (i.e., 500 or more), even if the breach does not pose any risk of impact or harm to the affected individuals. There seems to be little point to this, which renders it impractical.

One should assume that at most times, and perhaps practically all the time, the PDPC will have before it at least one data breach incident case that does involve material risk of harm to individuals and to which its staff should be paying close attention. It may be that the PDPC will always have before it several or many such cases. If an affected enterprise delivers to the PDPC a breach notification for an incident that involves 500 individuals but does not pose any risk of impact or harm to the affected individuals, the PDPC's staff might decide to handle the matters in the most resource-efficient manner possible, which is to ignore the breach incident that does not pose any risk of impact or harm, and focus instead on the breach incident that does, however smaller the number of affected individuals may be. This would be as it should be, because public service, in the form of preventing or mitigating harm to data subjects of and in Singapore, is much closer to the PDPC's mission than the bureaucratic processing of reports of past events that had no real-world consequences. The proposal in Section 6.2(b) would impose a burden on the PDPC's workload and a distraction from its mission of preventing or mitigating *actual* harm to *actual* data subjects.

To illustrate, if an affected enterprise delivers to the PDPC a breach notification for an incident that involves 5 million individuals but does not pose any risk of impact or harm to them, the PDPC's staff might decide to ignore the incident, and focus instead on other cases that do involve *actual* risk of impact or harm, even if "only" to 50,000 *actual* individuals. The PDPC's staff might decide to turn their attention to the accumulating backlog of cases that do not pose a risk of impact or harm only once there is a lull in breach incidents that do. But given that breach incidents are becoming ever more prominent and urgent with each year, this would perhaps be tantamount to turning to these cases only after they have become old and no longer relevant, or perhaps even never turning to them at all.

The same argument applies to the preceding criterion of Section 6.2(a). The obligation to report "any risk", even minor, immaterial and inconsequential risks, is an obligation to report for reporting's sake. It may inspire unnecessary fear or anxiety

Singapore Personal Data Protection Commission, at corporate@pdpc.gov.sg

September 21, 2017

Page 6

among the members of the general public who learn about minor, immaterial and inconsequential risks. It may inspire lawsuits against affected enterprises from members of the general public who learn about the breach after the notification has been made and become anxious. This risk of lawsuits practically by definition did not have to exist, because the breach did not involve any risk of impact or harm. Wiser is the approach taken in the new Australian breach notification framework, which requires breach notification only where a reasonable person would conclude that the breach *is likely to result in serious harm* to any of the individuals to whom the information relates.

There may be an argument that requiring affected enterprises to report data breach incidents that involve larger numbers of individuals but no risk of harm, or involve only minor, immaterial and inconsequential risks, would have the beneficial effect of compelling businesses to implement robust information security measures in order to avoid data breaches, if there were also a penalty for failing to report the breach in the form of a large fine or even a criminal penalty. I would suggest the argument is unavailing. To attach a heavy fine or criminal penalty to a failure to report is rather like criminalizing the fact of having been affected by a data breach incident. But the breach may have been the result of technological advances that made it easier for bad actors to breach defenses that once (or even recently) had been up-to-date, and to suppress or erase evidence of what they did and how. In the end, the breach is the result of malicious decisions and actions of the bad actor, and so it is the bad actor, not the affected enterprise, that actually deserves punishment. Penalizing a failure to report a data breach, particularly when the incident has no risk of harm, is rather like blaming an innocent person for something that never gave rise to a private cause of action, and would make Singapore appear a hostile or risky place to process data.

***Question 6: What are your views on the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations?***

This is in reference to Sections 6.3(a) and (b) of the Public Consultation Paper. I would suggest a different approach. This approach varies in concept only. In practice, it would have a result that is very similar to that of the existing proposal.

First: The PDPA was originally proposed as a baseline privacy law. That is to say, it was originally intended to provide a basic level of protection to all personal information, while recognizing that, within specific industry sectors, personal information could and should be handled and governed using industry-specific rules and regulations. It was for that reason, for instance, that the PDPA does not itself contain a definition of "sensitive personal information." The concept of "sensitive personal information" would be appropriate in some industry sectors but not in others. The various industry sector regulators would therefore determine for themselves whether they would, using sector-specific privacy regulations,

Singapore Personal Data Protection Commission, at corporate@pdpc.gov.sg

September 21, 2017

Page 7

establish a definition of “sensitive personal information,” and regulations for the collection and handling of “sensitive personal information,” for their own sector.

Data breach notification requirements are comparable to “sensitive personal information” in that respect, insofar as the urgency of the notification requirement, and the content that should be in the notice, may vary according to industry sector. For instance, an industry whose business activity collects only information that is already in the public record might be subject to very light breach notification requirements, if any at all. In contrast, an industry sector that involves personal health records or personal financial information may adopt more stringent breach notification requirements for incidents in which such information had been compromised.

Second: The idea that (1) the data breach notification rules of the PDPA and (2) the data breach notification rules of a specific industry regulation should *concurrently* apply has the potential to result in the need to conduct a complex inquiry. Where the two are exactly the same this inquiry is not difficult, and where they are completely contradictory this inquiry also is not difficult (because the sector-specific breach notification rules would prevail). What presents difficulty is where they are *similar* or *parallel*, yet *different*. In these instances the question of which to actually comply with, or how to synthesize the two sets of rules into a coherent whole, could well be a complex legal analysis that will involve parsing through many nuances and reconciling similar but still different phrasing.

The middle of a crisis situation is no place to be conducting this kind of subtle, nuanced and possibly even philosophical analysis. An enterprise in the middle of an information security crisis, with possible litigation and liability looming at the same time that it still may not have all information about the incident, does not have the luxury of undertaking that kind of analysis. Instead, it needs bright line, easy to read and easy to understand, executable and practically actionable directives.

For the foregoing two reasons, I would suggest that, where the affected enterprise is required to notify a sector regulator or law enforcement agency or affected individuals under other written law, and that data breach also meets the criteria for notifying the PDPC, instead of having the data breach notification requirements under the PDPA *apply concurrently* with the notification requirements under the other written law, the data breach notification requirements of the PDPA *should not apply*, and should *defer* to the data breach notification requirements of the specific industry regulation, which *alone* should prevail and apply. I should note that this would be consistent with the exclusion under Section 4 of the PDPA that would apply to the proposed breach notification provisions, under Section 6.9 of the Public Consultation Paper.

The sole modification to the data breach notification requirements of the specific industry regulation should be that the PDPC should receive in a timely manner a copy of any *written* notification that is delivered to the industry regulator. It would include only *written* notification, and would not require that the PDPC be notified *simultaneously with* the

Singapore Personal Data Protection Commission, at corporate@pdpc.gov.sg  
September 21, 2017  
Page 8

industry regulator, because the very first notification is sometimes made in person as a courtesy, and the members of the affected enterprise's breach response team are not likely to be available to notify both the PDPC and the industry regulator at the same time. They cannot be in two places at once.

Finally, having made this point, I would also make an additional suggestion that goes a step further. *The existing position of the PDPA, in which it does not itself contain a mandatory breach notification requirement, and leaves it to industry-specific regulators to impose their own sector-specific mandatory breach notification requirements if and as they see fit, has merit.* The existing position is true to the PDPA's original function and mission as a baseline law. The existing position allows industry regulators, who understand the circumstances prevailing in their industry sectors with particular familiarity, to make the decision as to whether to establish or not establish a breach notification requirement in their industry sector. This will result in sector-specific breach notification frameworks, each of which more accurately reflects the particular realities of each industry sector.

***Question 7: What are your views on the proposed exceptions and exemptions from the data breach notification requirements?***

This is in reference to Sections 6.9, 6.10 and 6.11 of the Public Consultation Paper. The proposed exceptions and exemptions do not present any problems. I would only suggest adding another two exemptions.

First: The affected enterprise should be given an opportunity to mitigate the likelihood of damages from the breach, and should be relieved of the obligation to make the breach notification if it has taken action that has rendered unlikely or not material (or not serious) the damages that may result from the breach.

Second: The affected enterprise should be relieved of, or permitted to delay, the obligation to make the breach notification if the breach incident is the subject of an ongoing or potential criminal investigation.

***Question 8: What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?***

The proposed time frame provided in to Section 6.13 of the Public Consultation Paper is not realistic. As explained above, the affected enterprise may not be in a position to notify within 24 hours (as in the UK) or 72 hours (as in the EU and as proposed for Singapore). That is because it may not have all of the information it needs to make an accurate breach notification. Making a rushed and inaccurate breach notification is not likely to help the data subjects, and from the affected enterprise's standpoint would result only in liability that did not have to exist in the first place.



Singapore Personal Data Protection Commission, at corporate@pdpc.gov.sg

September 21, 2017

Page 9

Rather than imposing a hard and fast, or arbitrarily short, breach notification deadline, I would suggest that the affected enterprise be allowed an opportunity to conduct an investigation into the facts and circumstances surrounding the information security breach incident, which includes an opportunity to assess the likelihood of risk and the types of risk involved. The affected enterprise should, subject to an opportunity to mitigate the likelihood of damages from the breach, be required to perform a notification requirement only where the risk of harm to a data subject appears likely and material. If the affected enterprise decides that a notification is appropriate, the notification to the PDPC should be required within 72 hours after the personal information controller has satisfied itself on the basis of its investigation that it has a clear understanding (a) of the nature and scope of the breach, including when and where it took place, (b) of the types and volume of personal information involved, (c) of the origin, source or reason for the breach and who may have caused it, (d) the number and identities of individuals who may have been affected, and (e) of the damages that are likely to result from the breach and what individuals could do to mitigate them. The affected enterprise's investigation in search of answers to these questions should not itself be subject to any particular deadline. In any case, the affected enterprise already has a strong incentive to notify affected data subjects as early as practicable after it has learned all of the facts, because it has an incentive to notify the data subjects before they learn of the incident from any other source (such as the press), so as to control the manner in which the story unfolds.

In addition, the affected enterprise should be given an opportunity to mitigate the likelihood of damages from the breach. I would suggest that if, at any time before the required time for the breach notification (i.e., 72 hours after the achievement of a clear understanding) the affected company has taken action to render unlikely or not material (or not serious) the damages that may result from the breach, the affected company should be relieved of the obligation to make the breach notification. This is consistent with the approach taken in the new Australian breach notification framework. The Australian approach is quite wise, because it enlists the affected enterprise in an effort to avoid harm to the data subjects, which is the important thing,<sup>2</sup> rather than leaving it in a situation where it will instead feel compelled to focus on analyzing strategies for responding to lawsuits from data subjects. It also gives it an incentive to start the process of mitigating risk of harm as early as possible after it has discovered the breach incident. In this way, it aligns the interests of the affected enterprise with the interests of the affected data subjects.

The proposed time frame provided in to Section 6.12 of the Public Consultation Paper is closer to the foregoing suggestion, and is more realistic. However, it still might present the practical difficulty of causing the affected enterprise to feel pressure to notify before it has a

---

<sup>2</sup> In the APEC Privacy Framework, the very first principle, prior to all the others, is Preventing Harm. See <https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group>.

Singapore Personal Data Protection Commission, at corporate@pdpc.gov.sg

September 21, 2017

Page 10

clear understanding of the facts surrounding the incident. I would therefore suggest that the foregoing suggested arrangement, of allowing the affected enterprise sufficient time to conduct and complete its investigation and arrive at a clear and confident understanding of the facts and circumstances surrounding the incident before being required to make any notification, apply *both* to notification of the PDPC *and of affected data subjects*.

\* \* \* \* \*

Singapore Personal Data Protection Commission, at corporate@pdpc.gov.sg

September 21, 2017

Page 11

## CONCLUSION

In conclusion:

1. If Singapore must have an overall mandatory breach notification requirement, I would suggest requiring notification only where there is a likelihood of material (or serious) harm. The mere number of affected data subjects should not trigger a breach notification requirement. The important consideration is whether the potential harm is likely or material (or serious).
2. If Singapore must have an overall mandatory breach notification requirement, I would suggest requiring notification only after the affected enterprise has had an opportunity to determine by means of an internal investigation (typically, a digital forensic investigation) what has happened. The affected enterprises should be given enough flexibility, in terms of the timing of the mandatory breach notification, to conduct and complete this investigation, and arrive at a clear and confident understanding of the facts and circumstances surrounding the incident before being required to notify.
3. If Singapore must have an overall mandatory breach notification requirement, I would suggest allowing the affected enterprise an opportunity to mitigate the risk, and relieving it of the breach notification obligation if it succeeds. Also, the affected enterprise should be relieved of, or permitted to delay, the obligation to make the breach notification if the breach incident is the subject of an ongoing or potential criminal investigation.