To: MICA_DP_Public_Consultation@mica.gov.sg

Subject: Hewlett-Packard's response to the Public Consultation of the Proposed Consumer Data Protection regime for Singapore.

Dear Sir/Madam,

We refer to the Consultation Paper on the Proposed Consumer Data Protection Regime for Singapore released by the Ministry of Information, Communications and the Arts (MICA) on 13 September 2011. We would like to thank MICA for giving us the opportunity to provide our feedback and comments to the proposed Data Protection (DP) regime.

Hewlett-Packard (HP) champions privacy and personal data protection because we see that protecting customer, client and employee personal data promotes trust and loyalty and, in turn, strengthens the HP brand. Good companies take their commitment to privacy seriously.

Even in the absence of any privacy or data protection legislation in Singapore, HP nonetheless respects and protects the personal information of customers, employees, and partners. Our worldwide privacy policies and practices create marketplace advantages, identify and help manage business risks, assure compliance with the law, and reinforce the company's reputation for ethical and values-driven business practices. The key milestones in HP's privacy policies and practices are as follows:

- 1997 – HP first launched its privacy program
- 1998 – HP created its privacy policy.
- 2001 – HP was the first technology company and first Fortune 500 company to self-certify with the Safe Harbor Agreement.
- Since 2005 – HP has been the sponsor of the HP-IAPP award which recognizes unique programs and services in global privacy and data protection across both private and public sectors.
- 2005 and 2006 – HP was awarded the Most Trusted Companies for Privacy Study by TRUSTe and the Ponemon Institute.

HP is also an advocate of customer privacy rights and is a forerunner of customer privacy rights initiatives. We have been actively involved in the following international forums:

- The Center for Information Policy Leadership: *Evolving Business Processes*
- SOM Privacy Sub-group: *Cross-border Rules, Accountability*
- Consumer Privacy Legislative Forum: *Unifying Federal Privacy Laws*,
- *Anti-Spyware Coalition, RFID Coalition*
- Privacy Officer's Network & Forum: *Accountability & BCRs, PRIME*

In addition to the above, HP has also participated in the following collaborations:

- Galway Project

- This is an initiative led by The Centre for Information Policy Leadership with Ireland's data protection commissioner to define the essential elements of an accountability model.

- Aside from HP, other participants include international experts from government, industry and academia.

- Privacy by Design: Essential for Organizational Accountability and Strong Business Practices

  - This is an article co-authored by the HP Privacy Officer and published in November 2009, in which HP's accountability approach is used as a case study.

- Accountability as a Way Forward for Privacy Protection in the Cloud

  - Research paper co-authored by HP scientist which proposes a combination of procedural and technical methods for resolving privacy and security risks in cloud computing.

HP supports legislation that protects legitimate privacy interests and rights. Such legislation can be of great benefit to the country, to its citizens, to the government as well as to businesses. However, if privacy requirements are implemented in isolation without due consideration to business impact and global interoperability (i.e., compatible requirements across countries or regions), international business and commerce would be inhibited.

It is therefore important for regulators around the world to set forth requirements that are easily understood, consistent and compatible with other countries' privacy laws so as to not introduce undue burdens on businesses. New privacy regulations should also take note of the experiences elsewhere – adopting beneficial privacy requirements and not repeating the mistakes of existing regimes.

Having reviewed the proposed DP regime, we are of the overall view that the proposed DP regime is extremely well thought out. We appreciate that MICA has thoroughly researched the various data protection regimes that have already been established in various other Commonwealth jurisdictions, and has applied the strengths of such data protection regimes to the specifics of our local jurisdiction.

However, notwithstanding the overall robustness and completeness of the proposed DP regime, we do have some comments that we would like to raise for MICA's consideration. We would be delighted to discuss matters regarding privacy and data protection in more detail. We trust that our experience in implementing our privacy policies and practices over the years; and our participation in various international forums and collaborations on privacy (as outlined above) may prove useful in the introduction of the proposed DP regime. Please feel free to contact us at your convenience.

Yours sincerely,

Allan Paull
APJ Privacy Officer

Hewlett–Packard's comments to
Ministry of Information, Communication and the Arts
Consultation paper of the proposed Data Protection regime

Introduction

HP would like to compliment MICA on its publication of the *Consultation paper of the proposed Data Protection (DP) regime* (the consultation paper) and for the comprehensive process taken to seek feedback from interested parties to the proposed DP regime for Singapore.

HP supports the balanced approach that MICA is taking in looking at ways to introduce effective data protection regulation that attempts to protect consumer interests and improve the understanding of consumer rights, while at the same time not imposing regulation that may inhibit business innovation, opportunities and ability to conduct business across country borders.

MICA's research into existing country data protection regimes around the world in order to identify and learn the lessons encountered by other countries is to be applauded, as the consequences of poorly drafted data protection regulations may adversely affect specific business sectors (as occurred recently in India after they introduced data protection "rules" that threatened their outsourcing businesses). Countries who adopt data protection requirements that differ significantly from their major trading partners (in particular if they are more onerous) may find that these requirements inhibit certain business operations. It is often that countries introduce data protection regulations without due consideration of the potential consequences.

Comments on the proposed Data Protection (DP) regime

While HP agrees with the majority of the recommendations expressed in the consultation paper we do however have the following comments that we would like to make in the hope that they may prove helpful:

1. ***Should DP law extend to organizations located outside Singapore***

HP agrees with MICA's analysis on the practical challenges around the enforcement of the proposed DP regime against persons or entities which do not have a physical presence in Singapore.

One proposed solution would be to adopt the Australian position, so that the proposed DP regime would apply to organizations located outside of Singapore which collect and process data only if both of the following criteria are satisfied (a) the personal information relates to a Singapore citizen or a person who is present in Singapore without any limit in time; and (b) the organization is Singaporean linked (with a clearly defined set of criteria to define what "Singaporean linked" means). In this way, there would both be a locus for enforcement (since the data is in relation to a person that has nexus to Singapore), and an ability to enforce against such organizations (since the organization is linked to Singapore).

MICA should also consider whether the proposed DP regime is applicable to the processing of personal data of individuals located outside Singapore. This will have a direct impact on the HP's outsourcing business, where HP processes personal data of individuals located outside Singapore under a contract with an organization located within or outside Singapore. In this regard, MICA should consider the significant concerns raised by the outsourcing industry in India with regards to the recently issued Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 ("**Rules**") in India and the subsequent clarification issued by the Ministry of

Communication and Information of Technology, which among others, clarified that (1) the Rules only apply to body corporate or any person located within India; and (2) the data collection and consent requirements do not apply to Indian organizations receiving sensitive personal data under a contract with any legal entity located within or outside India. This means that a non-Indian organization that outsources the processing of personal data to an organization in India, need not comply with the data collection and consent requirements under the Rules and neither should their service provider in India. We feel that the approach taken by the Indian Ministry of Communication and Information of Technology is in line with MICA's intent of creating a conducive environment in Singapore for a fast-growing global hub data management and data processing.

2. Comments on the proposed general rules under the DP law

In paragraphs 3.28 to 3.30 of the consultation paper, it is stated that the proposed DP regime would not distinguish between the concepts of "data controllers" and "data processors". The essence of the application of the proposed DP regime is set out in paragraph 3.28 of the Consultation Paper, where it is stated that an organization will be held responsible for "*personal data under its custody or control,* including *personal data that is not in the organisation's custody but is under its control.*"

Under the proposed DP regime, an organization that merely processes data is still likely to be deemed as having control over any personal data that it processes. A more direct interpretation of the statement of application above would be that as an organization is responsible for personal data under its custody **or** control, an organization that processes data would necessarily have the data under its custody (though not necessarily under its control) and would thus fall within the jurisdiction of the proposed DP regime.

HP would request MICA to consider drawing a distinction between data controllers and data processors in future data protection legislation. The reality of the situation is that such organizations as data processors do not collect the data (and have no ability to comply with obligations relating to collection, use, access, disclosure etc) and have no actual control over the data that they are processing. Even worse, it is also often the reality that such organizations have no knowledge of what data it is they are processing. Thus, in actuality, the control over the data is in the hands of the data controller, not the data processor.

Take for example an organization who owns facilities that house data storage equipment (**"Organization A"**). Another organization that owns data storage equipment is in the business of providing data storage services (**"Organization B"**). Organization B leases facilities from Organization A to situate its data storage equipment. Organization B then provides data storage services to an organization that has actual control over personal data (**"Organization C"**). Organization C stores the personal data that it controls on Organization B's storage equipment. In this scenario, Organization C is the organization that has actual control over the personal data and should be subject to the Regime. However, it is arguable that Organization A and Organization B may both be deemed to have custody or control over the personal data as the personal data is contained both within Organization B's equipment and Organization A's premises. However, it would not be economically viable for Organization A and Organization B to scrutinize each and every piece of data stored in its premises or equipment (as the case may be) to ascertain (a) if such data constitutes personal data; and (b) if such personal data was properly collected with consent pursuant to the Regime.

A related concern arises in the situation where the organization is collecting and processing the data from residents of other countries on behalf of another company. For example a Singapore organization may be hired by an organization in the European Union (EU) to collect and process personal data on

their behalf. The EU based organization may require the Singapore organization to comply with requirements from the EU Data Protection Directive. The issue arises when there may be significant differences between the EU Data Protection Directive and the proposed DP regime. These may be in conflict and as a result create a dilemma for the Singapore organization about which requirements (Singapore or EU) should apply to the data they are handling.

A parallel situation to the examples above can be seen in relation to Network Service Providers (**"NSPs"**) and the Copyright Act in Singapore. NSPs in relation to the Copyright Act are caught in a similar situation as organizations that provide data processing services in relation to the proposed DP regime. NSPs own the equipment that transmit and store information on their networks, and hence can be construed to have control and/or custody over such information. However, it is an actual fact that NSPs cannot be expected to have full knowledge of what information is being stored and/or transmitted over their networks. Likewise, it must be recognized that NSPs do not have real control over such information as well. NSPs will also have to be careful in identifying which laws they are expected to comply with, given the global nature of the Internet and other networks.

The Singapore Parliament recognized the realities of the situation when enacting the Copyright Act, and NSPs were specifically provided with a "Safe Harbour" in the Copyright Act, where NSPs would not be found liable for infringing information found on their networks so long as certain criteria have been met.

Aside from the implementation of "Safe Harbour" rules, as noted in paragraph 3.28 of the Consultation Paper, other jurisdictions such as the European Union tackle this problem by differentiating between a "data controller" and a "data processor" and applying differentiating standards to both. Under the Canadian regime, there is an onus on the organization engaging the services of a third party data processor to use contractual means to ensure that personal data is being afforded a comparable level of protection while being processed.

All things considered, we are of the view that the current proposed application of the proposed DP regime to organizations that merely process personal data does not take into proper consideration the realities of the situation – that such organizations do not have the requisite knowledge and control to be in a position to comply with the requirements of the DP regime.

We strongly urge MICA to consider implementing instead the EU approach of separate definitions of "data controller" and "data processor" and to apportion obligations under the proposed DP regime accordingly. Alternatively, the Copyright Act approach of implementing a "Safe Harbour" for organizations that merely process data on behalf of another organization without control over the data can also be considered.

3. Accountability and consent

HP feels that a data protection regime's reliance on user consent for organizations to use and process personal data may over time prove problematic and Singapore might miss an opportunity to explore the recent developments and trends toward privacy accountability that are taking place around the world. For instance Mary J. Culnan Slade Professor of Management and Information Technology at Bentley University contends that *"the current approach to regulating privacy based on "notice and choice" or "harm" is not effective and needs to be revisited. This approach places too much burden on the individual, frequently deals with harm only after the fact, and has failed to motivate organizations to*

proactively prevent privacy or security incidents resulting from their information processing activities" [1]. Her proposal is create new regulations based on accountability where organizations create risk management programs reflective of their circumstances.

The reference to accountability in the context of an organization may include the following:

- exhibiting transparency;
- being committed to privacy and data protection;
- being able to effectively demonstrate that it can meet the promises it makes regarding privacy and data protection;
- building and implementing infrastructure and programs to carry out such promises and commitments; and
- continually monitoring, verifying, and validating that the infrastructure and programs work effectively.

Most approaches to privacy or data protection regulation have tended to be designed around providing notice of how the data may be used etc. and whether consent or choice will be offered to the individual about this use. Notices originally intended to aid an individual have become complicated legal documents designed more to protect the organization, with the result that quite often they are difficult to comprehend and understand.

Another issue is that regulation has rarely been "in front of the curve" and has tended to follow technological or informational developments and practices constantly trying to keep pace and often becomes out of date with current data handling practices.

With the constant evolution of new technology and new forms by which individuals and businesses interact and communicate (such as with the advent of social media and cloud computing), it is important to move the focus of an organization's commitment to privacy and data protection from one of merely "user consent" to a framework of overall clear accountability. DP regulations should not overly emphasize the issue of user consent, but instead require organizations to have clear accountability of the measures they have in place to ensure that they meet their commitments towards ensuring consumer privacy and data protection. For example, requiring organizations to have in place a comprehensive assurance program may be appropriate in ensuring an organization's accountability in consumer privacy and data protection.

HP, in collaboration with the Centre for Information Policy Leadership, has developed an accountability model framework that helps our employees assess and manage the risks associated with collecting and handling personal data, going far beyond legal requirements to ensure that employees handling data are accountable and that their practices are transparent. We have developed sound policies aligned to external criteria, we have the mechanisms and tools (such as our Privacy Advisor tool) to help ensure our policies and commitments are given effect and we have introduced monitoring and assurance programs and measures that validate both coverage and effectiveness of data handling within HP.

We would be glad to discuss this issue of accountability further with MICA, and to share our experience in implementing our accountability model framework and the various mechanisms and tools we employ

[1] Accountability as the Basis for Regulating Privacy: Can Information Security Regulations Inform Privacy Policy? Mary J. Culnan Slade Professor of Management and Information Technology IPM Department Bentley University July 2011.

to assist MICA in developing a suitable accountability framework for organizations under the proposed DP regime.

Designation of individuals

In relation to the identification of specific individuals who will be responsible for ensuring the organization complies with the proposed privacy legislation, HP feels that this may not always be practical, and individuals within the organization may constantly move or change roles or leave the organization, quickly dating any contact details that may be publicized. We therefore propose that instead of requiring organizations to designate a specific individual or individuals, MICA consider also permitting the organization to publicize the designated groups within the organizations responsible for data protection compliance and the contact details of such groups. One example of such a designated group is HP's Chief Privacy Office.

Further to the above, it is not clear from the consultation paper what exactly is the extent of liability that such designated individuals will have to bear. From the consultation paper, it appears that the individuals are to bear responsibility for each organization's adherence to the proposed DP regime, with the organization also bearing responsibility in the event of breach. This may be construed to mean that the designated individuals may be personally liable in the event they fail to ensure that their organization complies with the proposed DP regime. This is contrary to the typical legislative approach on privacy laws and the way most organizations are operated. HP proposes that the wording of the section be revised to provide more clarity on the liability (if any) that such designated individuals would bear under the proposed DP regime. HP further proposes that no personal liability be borne by such designated individuals, and that the organizations should solely bear the liability for breach.

Consent

In relation to the issue of consent, we note from paragraph 3.32 of the consultation paper that the proposed DP regime would not prescribe in detail the manner in which consent may be given. Consent may be explicit or implied, depending on the circumstances.

We are of the view that it is of utmost importance to organizations that implied consent be sufficient for organizations to be permitted to collect, use and/or process personal data under the proposed DP regime. This would greatly reduce the implementation costs for organizations, as to obtain explicit consent from each and every data subject (and to retain evidential records of such explicit consent) would be costly and onerous on organizations.

We would like to highlight that individuals are always protected under the proposed DP regime. As an example, in the unlikely event that an organization misconstrues an implied consent, the individual concerned may at any time, unilaterally withdraw any such implied consent that may have been given, in which case the organization would be deemed to no longer have consent to collect, process or use the personal data of the individual.

We are reassured that MICA has given fair consideration to the difficulties faced by organizations in having to obtain explicit verbal or written consent when collecting, processing or using personal data, and that MICA has decided to include implied consent within the definition of consent for the purposes of the Regime.

One query that we would like to raise, is whether consent may be implied from an opt-out procedure during a data collection exercise. For example, the data subject's attention may be drawn to a section

stating that the data would be collected, processed and/or used (i.e. the required disclosure), and that the data subject should indicate in writing if it did not consent to such collection, processing and/or use by way of a provided checkbox. If the data subject were to leave the checkbox blank, then would an organization be able to rightfully construe the same as implied consent?

4. Transfer of personal data outside Singapore

HP supports the proposal to allow the transfer of personal data outside SIngapore and the adoption of a "principle based" approach with respect to the transfer of personal data where the onus will be on the organization transferring personal data out of Singapore to ensure that the organization to whom personal data will be transferred implement appropriate measures to protect the personal data. This approach should ensure that Singapore's DP regime will be consistent with APEC's Cross-Border Privacy Rules system.

5. Retention period when collecting personal data

Specifying exact retention periods may prove difficult as organizations may collect personal data in the course of business that has vastly different uses or purposes and as a result may need to be retained for different periods of time. In addition some laws require data to be retained for specific periods of time which makes it difficult for organizations to try and differentiate which personal data to retain and which to delete. Lastly, as not all countries impose specific retention periods, organizations in Singapore may find it difficult processing personal data on behalf of clients in other countries who do not impose such requirements.

6. Suggestions on specific guidelines that the DP Commissioner should provide

From experience, HP has found that data protection regulations are set at a high compliance level and tend to be general in nature. Hence, guidance on the operation and interpretation of the data protection laws are important. As an example, in Australia, the Federal Privacy Commissioner provides comprehensive guidance on different aspects of the Privacy Act through "Information Sheets", "Guidelines to the National Privacy Principles" etc. HP feels that the DP Commissioner be given similar responsibilities in order to assist organizations comply with the DP regime.

7. Transitional Arrangements

HP supports MICA's proposals for a reasonable transition period that will afford organizations a grace period to prepare themselves and make necessary internal changes to comply with the DP Act.

8. Existing personal data

HP agrees with MICA's proposal that the DP Act should not have any retrospective applicability to existing personal data.

9. The proposed National Do-Not-Call Registry

<u>Residential numbers</u>

HP suggests that any requirements relating to the National Do-Not-Call Registry should apply only to residential numbers in Singapore (similar to existing Do-Not-Call legislation in Australia) and should not unduly restrict businesses from legitimately making contact with customers with whom it has an existing business relationship.

<u>Opt-out rather than Opt-in</u>

We agree that that the proposed National Do-Not-Call Registry should be premised on the basis of individuals having the ability to "opt-out" instead of a blanket restriction against telephone marketing, or requiring individuals to specifically "opt-in". This will allow organizations to pursue their telemarketing activities, individuals to continue to benefit from being informed about new products, services or promotions and provide options for those who would otherwise prefer not to be contacted. We strongly urge MICA to retain this "opt-out" approach in the event MICA decides to implement the National Do-Not-Call Registry.

Reasonable Lead Time

It will be worthwhile of MICA to clarify its expectations in relation to the frequency at which organizations are expected to check the registry and the time given for them to update their own records and to cease contacting registered individuals and the associated penalties involved in non-compliance.

It is unrealistic to expect organizations to update themselves with the National Do-Not-Call Registry on a real-time basis prior to each and every a marketing call, SMS or fax. There will necessarily be a time lapse between the time an individual registers with the National Do-Not-Call Registry and an organization updates itself with the latest information within the National Do-Not-Call Registry.

One solution to this problem would be the implementation of a technological measure that MICA can provide to organizations that would push the contents of the National Do-Not-Call Registry to all organizations on a real-time basis whenever the National Do-Not-Call Registry is updated. However, the implementation of such technological measure must be cost and time efficient, and has to be versatile enough to integrate with the myriad of technological systems used by organizations in Singapore. Further to the above, exceptions would have to be made to the proposed DP Regime for instances where the technology fails to update the organizations in good time. In such an event, liability for failure to comply with the National Do-Not-Call Registry should not fall on the organizations.

An alternative solution would be to provide a lead time between the registration of an individual on the National Do-Not-Call Registry, and when organizations are expected to cease making unsolicited marketing contact with such individual. This would give organizations reasonable time to update themselves with the latest information within the National Do-Not-Call Registry.

In this regard, our proposal is that the registration of an individual on the National Do-Not-Call Registry should be effective the calendar month following his or her registration, provided that he or she registered at least five (5) calendar days before the last day of the month. In the event the individual registers during the last five (5) calendar days of the month, then his or her registration should be effective two (2) months from such registration. This would allow organizations to schedule their Do-Not-Call register updates during the last five (5) calendar days of each month to generate their updated telephone marketing target lists for the following month.

Conclusion

In conclusion, HP believes that the approach MICA has taken in initiating the process to develop the new DP regime for Singapore is encouraging and we hope that these comments and suggestions may be of value in shaping the development of the new DP regime. If MICA intends to establish working groups to review specific aspects of the data protection regime, HP would be keen to participate and share its experience.

If you have any questions or would like to discuss this further please don't hesitate to contact:

Allan Paul, APJ Privacy Officer

DID No: +61-411-232-249

Email address: allan.paull@hp.com

Lye Yi Xiang, Legal Counsel, Office of the General Counsel

DID No: +65-6572-3967

Email address: yi-xiang.lye@hp.com

References:

1. Accountability as the Basis for Regulating Privacy: Can Information Security Regulations Inform Privacy Policy? Mary J. Culnan Slade Professor of Management and Information Technology IPM Department Bentley University July 2011.