THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

HUNTON & WILLIAMS LLP
2200 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, D.C. 20037

TEL 202 • 955 • 1500
FAX 202 • 778 • 2201

MARTIN E. ABRAMS
DIRECT DIAL: 202 • 778 • 2264
EMAIL: MABRAMS@HUNTON.COM

PAULA J. BRUENING
DIRECT DIAL: 202 •955 •1803
EMAIL: PBRUENING@HUNTON.COM

October 24, 2011

VIA Electronic Mail Delivery

Ministry of Information
Communications and the Arts
Singapore Government
140 Hill Street #02-02
MICA Bldg, Singapore 179369

Re: Public Consultation Issued By Ministry of Information, Communications and the Arts on its Proposed Consumer Data Protection Regime for Singapore

Dear Sirs and Madams:

The Centre for Information Policy Leadership appreciates this opportunity to comment on the Ministry of Information, Communications and the Arts' (MICA) public consultation document regarding its Proposed Consumer Data Protection Regime for Singapore. The Centre commends the Ministry for its decision to address the timely and challenging issues raised by the dynamic evolution of the information economy.

The Centre's mission is development of forward-thinking information policy that encourage both privacy and innovation in a digital economy. It has led projects addressing numerous information privacy and security issues including privacy notices, global flows of data, accountability-based governance, development of privacy law in emerging economies, and government's use of private sector data. The Centre has worked extensively with business, advocates, experts, congressional staff and international organizations on issues of privacy and data protection.

The Centre was established in May 2001 by leadership companies and Hunton & Williams LLP. It is located within the law firm of Hunton & Williams and is financially supported by approximately 40 member organizations. The Centre's views and the views expressed in this response are its own and do not necessarily reflect those of its member companies, the law firm of Hunton & Williams LLP, or the firm's clients.

I. Summary

The Centre for Information Policy Leadership commends MICA for undertaking this inquiry, and submits the following comments on the Proposed Consumer Data Protection Regime for Singapore:

- The consultation paper appropriately recognizes the growing complexity of data collection and use, and of the business models and technologies that support these activities.
- It also acknowledges the limited ability of consumers to keep pace with rapid changes in the way data is collected, used and stored.
- We agree that in this dynamic environment, choice is of limited effect as a means for consumers to safeguard their privacy. Moreover, while choice is still important in some circumstances, individuals have less and less control over many aspects of the use of their data.
- In spite of these changing circumstances, the consultation paper properly notes that the burden lies disproportionately with the individual to police a complex marketplace and protect against the inappropriate use of data.
- We are concerned that in spite of this recognition, the consultation document proposes reliance upon consumers' complaints to bring regulators attention to misuses of data. Such an approach would not alleviate the burden on the consumer.
- Furthermore, the consultation document anticipates a data protection regime that relies significantly on consent to determine how data may be used by organizations. However, adequate notice for consent may in some cases not be possible, and obtaining consent may not be feasible.
- We suggest a use-and-obligations approach that relies upon the manner in which data is to be used, rather than its collection, to determine the organization's obligations with respect to data management.

- We further recommend that Singapore adopt an accountability approach to data governance that would require that organizations implement comprehensive programs to put privacy principles into effect, and be prepared to demonstrate those programs if asked by the data protection authority.

II. Comments

The consultation paper appropriately recognizes the growing complexity of data collection and use, and of the business models and technologies that support these activities. It also acknowledges the limited ability of consumers to keep pace with rapid changes in the way data is collected, used and stored.

We agree with the paper's assertion that in this dynamic environment, informed choice about the manner in which data is used is of increasingly limited effect as means by which consumers might safeguard their privacy. The rapid change, proliferation and complexity of new technologies and business models challenge the ability of even sophisticated consumers to keep pace and make sense of the ways in which data is collected, stored, shared and used. Privacy policies, which are expected to serve as the basis for choice, are ill-equipped to provide consumers with the information necessary to make informed decisions about the use of their data. In light of these changing circumstances, the consultation properly notes that the burden lies disproportionately with the individual to police a complex marketplace and safeguard against the inappropriate use of data.

Moreover, while choice is still important in some circumstances, individuals in fact have less and less control over many aspects of the collection and use of their data. Data has become so essential to individuals' engagement in public life, choice about its use remains meaningful in increasingly fewer situations.

We are concerned that in spite of this recognition, the consultation document suggests that Singapore's proposed data protection regime rely upon consumers' complaints alone to determine against which organizations it will enforce. Rather than alleviate the individual's responsibility to safeguard their data and privacy in a highly complex environment, such an approach would continue to impose on him the burden of understanding in detail an organization's privacy policies and promises, and recognizing when it acted outside the boundaries of law, regulation and organization policy. The Centre suggests that, even in the absence of consumers' complaints, data protection authorities should be empowered to initiative investigations based on their own review of the marketplace.

Furthermore, the consultation document anticipates a data protection regime that relies significantly on consent to determine how data may be used by organizations. Obtaining

consent, however, has become increasingly difficult. Adequate notice may in some cases not be possible at all (in cases of surveillance of public spaces, for example, or in use of facial recognition technology), and obtaining consent for use of such data may not be feasible. The Centre suggests that MICA consider a different model that relies upon the manner in which data is to be used, rather than its collection, to determine the organization's obligations with respect to data management.

The use-and-obligations[1] model establishes the use rather than the collection of data as the primary driver of a data collector's obligations related to notice, choice, and access and correction. It does not supplant established and well-respected notions of fair information practices, but rather provides a method for their application that better reflects the realities of the 21st century data environment. Under current implementation of fair information practices, consumer choice or consent to use data in certain ways establishes a company's responsibilities. A use-and-obligations model shifts responsibility for disciplined data use to the data collector and all holders (e.g. third party vendors) of data, imposing requirements for transparency and notice, consumer choice, and access and correction on the data collector based upon the way the data is to be used.

The model takes into account all of the *uses* that may be required to fulfill the consumer's expectations and meet legal requirements. It imposes on organizations obligations based on five categories of data use: 1) fulfillment, 2) internal business operations, 3) marketing, 4) fraud prevention and authentication, and 5) external, national security and legal. The purpose for which the data is to be used determines the organization's obligations to apply fair information practices.

The use-and-obligations model recognizes two aspects of a company's *obligations*, as articulated in fair information practices. The first includes the actions organizations must take to facilitate individual participation — transparency (notice), choice, and access and correction. These ensure that an individual can know what data about him an organization is collecting or holds; can make choices about its use when practicable and appropriate; and can access and correct it in appropriate circumstances. The second includes the internal steps an organization takes to effectively manage data to minimize risk to both the organization and the individual — collection limitation and data use minimization; data quality and integrity; data retention; security; and accountability.

[1] The use-and-obligations model is described in full in the document "A Use and Obligations Approach to Protecting Privacy," December 2009, attached as Appendix A and available at http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf.

We further recommend that Singapore adopt an accountability approach to data governance. Accountability[2] requires that organizations implement comprehensive programs to put privacy principles into effect, and be prepared to demonstrate those programs if asked by the data protection authority. It works in tandem with a use-and-obligations approach, making organizations responsible and answerable for the decisions they make about how best to meet their obligations to protect and manage personally identifiable data found in law, regulation and public policy. Accountability is designed to provide robust protection for data while avoiding aspects of current data protection that may be of limited effect or that may burden organizations without yielding commensurate privacy benefits. It allows the organization greater flexibility to adapt its data practices to serve emerging business models and technologies and to meet consumer demand. In exchange, it requires that the organization commit to and demonstrate its adoption of responsible policies and its implementation of systems to ensure that those policies are carried out in a way that protects information and the individuals to which it pertains.[3] Furthermore, accountability addresses concerns raised in the consultation document about the appropriate reach of Singapore law. Accountability requires that collectors and users of data remain responsible and answerable for the protection and management of data, no matter where or by whom it is processed. An accountability-based approach to data governance focuses on setting privacy-protection goals for organizations based on criteria established in current public policy and allowing organizations discretion in determining how those goals are met. Accountable organizations will adopt methods and practices to reach those goals in a manner that best serves their business models, technologies, and the demands of their customers.

---

[2] A comprehensive discussion of accountability can be found in "Data Protection Accountability: The Essential Elements," October 2009; and in "Demonstrating and Measuring Accountability," October 2010. Further information about accountability will be available in "Implementing Accountability in the Marketplace," to be released in early November 2011. These documents are attached as Appendix B and at http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf and http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF, respectively.

[3] Accountability is the first principle in Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"), requiring that Canadian organizations put into effect the full complement of PIPEDA principles, whether the data are processed by the organization whether the data are processed by the organization or outside vendors, or within or outside Canada. It provides that every organization must be accountable for its compliance with the requirements of the Act. "The Future of Privacy," the joint paper of the European Union Article 20 Data Protection Working party and the Working Party on Police and Justice, notes the significance and utility of the accountability principle, and cites the challenges to data protection raised by globalization and new technologies as offering an opportunity to "innovate the current legal framework by introducing principles such as accountability." http://www.garanteprivacy.it/garante/document?ID=1707337. In a later Opinion on accountability submitted to advise the European Commission about how to amend the Data Protection Directive, the Article 29 working party defined a statutory accountability principle to "explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request." http://ec.europa.eu/justice/policies/privacy/docs/2010wp173_en.pdf.

An accountability approach is already suggested in Sections 3.28 and 3.29 of the consultation document. These sections state in relevant part: "The proposed DP law does not distinguish between organizations as data controllers or data processors, but will hold an organization *responsible for personal data under its custody or control, including personal data that is not in the organizations custody but is under its control. . . An organization that outsources the collection and/or processing of personal data is still responsible for the management of such personal data.*"

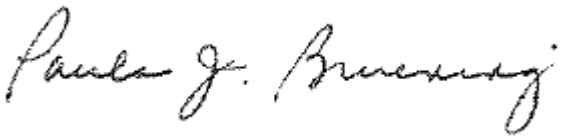
Moreover, Section 3.61 suggests a "principles-base" approach to cross-border data transfers, in which the onus will be on the organization to ensure that appropriate measures are taken to protect personal data where such data is transferred outside Singapore, as the organization is considered to have control over the data. The Centre encourages MICA to pursue this approach further, and consider its application not only to cross-border transfers, but to the data protection framework as a whole.

III. Conclusion

The Centre for Information Policy Leadership is pleased to have had the chance to comment on proposals for a Singapore data protection regime that would meet the challenges of 21st century data economy, protecting individuals and encouraging flexible, innovative data use. It encourages MICA to continue to explore emerging approaches to data protection and is available as a resource to MICA as it continues this important work. Please direct any questions to Martin Abrams at mabrams@hunton.com or Paula Bruening at pbruening@hunton.com.

Yours sincerely,

Martin E. Abrams
President



Paula J. Bruening
Vice President, Global Policy