A Member of Public's Commentary on the Proposed Consumer Data Protection Regime for Singapore

Mr Adam Reutens-Tan

I. Introduction

Firstly, I commend the Ministry for Information, Communication and the Arts (MICA) on exploring a more in-depth Data Protection Regime for consumers here in Singapore.

In an increasingly interconnected world, where members of the public are constantly either forced to give their particulars for a variety of services or products, or provide them willingly through their own social media, there definitely needs to be more extensive and comprehensive protection measures to ensure that the data remains secure.

II. Driving Purpose for Data Protection

I feel that MICA needs to determine the primary reason driving the implementation of the data protection regime. Would it be to help prevent identity theft, where hackers could gain access to an individual's private data and use it for their own gain? Or perhaps prevent con artists from simply buying a database of contacts and extract private information from gullible consumers?

Or would the data protection regime seek to prevent organisations and individuals from invasively reaching out to consumers to market their products and services?

The main question is this: are we protecting the consumer's data or privacy?

I feel that there would be many driving reasons, which would necessitate a tiered approach to the scope and depth of the protection.

III. Scope and Depth of Protection

For example, certified and registered medical bodies should have access to a wider range of data and information on their client, which could be accessed by other such medical bodies as necessary. Such information could be about their client as well as their client's family, to treat certain ailments or to inform them of their client's condition. And in some cases, say for a client who is not necessarily in charge of his or her full faculties, this information could be accessed and used without the client's express consent.

I feel that a main determinant of the availability of a consumer's data is dependent on two factors: necessity.

To elaborate, is the access and use of the information necessary for the consumer's continued livelihood and/or well-being? And if so, to what extent and to whom should the data be made available?

For instance, I feel that organisations are needlessly collecting a plethora of information from clients: from mobile numbers and email addresses to birth dates, NRIC numbers, credit card numbers and more.

Some of these are not required for the organisation, usually a commercial enterprise, to fulfill its customers' needs and wants through its products and services. So the data protection regime should already enforce a limit on the mandatory collection of data to the minimum required for a company to adequately perform its duties. Other unnecessary information should be clearly indicated as optional information to be given at the consumer's discretion.

Secondly, such data as collected from and on clients should be securely stored and accessed only be key individuals for the sole purpose of serving its consumers/clients.

For instance, medical records could be shared only between medical professionals who will both be acting to directly serve the patient. This information would be between individuals, not medical institutions, and only information necessary for the patient's treatment would be shared.

Likewise, a commercial organisation collecting information on its customers, whether through the product warranty, a contest form or some other means, should ensure that the data remains solely within its access and control, with said access being limited only to individuals who may need that access to ensure that the customers' needs are met.

The only exception to these rules would be data collection companies who must be very clear in explaining to the consumers that the data collected, or mined, from and on them will be used by other companies.

Basically, NO commercial organisation, save for data collection companies, should ever:

- collect data that is not essential for them to serve their customer/client/patient;
- release the data they have on their consumers, whether for commercial gain or not, without first explaining the purpose of the release; and/or
- release said data without the consumers' explicit consent.

Another area for data protection should be information that a consumer him or herself makes publicly available, whether through social media, a personal website or other means.

Such data should be protected from use by all external parties for their own direct or indirect gain. There are already intellectual property rights that safeguard ideas and works released by the author into the public domain; more stringent safeguards should exist for personal data.

IV. National Do-Not-Call Registry

MICA has proposed a National Do-Not-call Registry which consumers can opt to register for, in order to avoid getting marketing solicitations via calls, faxes and SMSes.

Definitely this is a good move, as consumers seek and value their privacy in a world that is becoming increasingly open. However, many consumers may not realize that option or know how to opt-out.

I would like to propose that the Registry be set up as a Can-Contact Registry (CCR), of consumers who are genuinely interested in having their data made publicly available. This is based on the premise that privacy is an inalienable right of the individual. As such, it should be up to the individual not whether to prevent his or her data from being used or exploited, but whether he or she should even allow his or her data to be accessed.

Within the CCR, individuals who have opted in can then have the freedom to select what types of information they would not mind having released, and to what kinds of organisations.

For example I might make only my name and address available only to real estate agencies, or my next of kin contact information available to insurance companies and medical agencies.

As the DP Public Consultation Paper, “telemarketers will benefit by being able to effectively target a genuine group of consumers who are interested in receiving information on the organisation‟s products/services, and eliminate time and resources wasted on those who do not wish to be disturbed.”

V. Public Education

Finally, MICA needs to educate the public to ensure that they understand their rights with regards to their data, the potential merits and dangers of making information publicly or selectively available, and how they can use the CCR.

VI. Conclusion

As I mentioned in the beginning, MICA has taken a step in the right direction with the advocacy of a Data Protection regime. It just needs to address the concerns and needs of the public whose data it is trying to protect, before it implements this regime.

<END>