COMMENTS ON SB NO. 2965 and HB NO. 4115:

AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES

Introduction

The Asia Internet Coalition (AIC) is an industry association founded by eBay, Google, Nokia, Skype and Yahoo!. Incorporated in Hong Kong, the AIC seeks to promote the understanding of Internet policy issues in the Asia-Pacific Region.

As an industry association representing global Internet players, the AIC hopes to be a responsible and relevant partner as the Conference Committee finalizes the Data Privacy Act. It is from this perspective that the AIC offers its further comments on the amendments agreed upon by the conferees and recommended in the Conference Committee Report.

Specific Comments

SEC. 3 – Definition of Terms

b.) Consent of the data subject – The Conference Committee drafting adopts the Senate version with some modified language. Of most concern to AIC members is the substitution of the wording **"MAY BE EXPRESS OR IMPLIED AND"** with **"SHALL BE".**

The consequence of this amendment is to establish a strict requirement for express consent which in all cases must be supported by evidence and precludes "implied" consent for processing of data.

As most data processing through websites is on the basis of implied consent to practices stated in privacy policies or other parts of a website the drafting of this provision will render most websites in breach and subject to criminal penalty.

The AIC submits that such an emphasis on express consent evidenced by written, electronic or recorded means over other existing alternatives of obtaining implied user consent presents a significant number of challenges in the era of big data and information technology. We believe that a regime that will impose a requirement for intrusive and disruptive requests for express consent (for example in the form of multiple pop-ups, check-boxes and additional mouse clicks) will not achieve the desired goals of protecting data privacy while promoting innovation and growth as declared in Section 2 without causing serious disruption to users' online experience. Faced with multiple requests, users rarely consider or understand the choices that they are making. Accordingly, requiring that consent be express will not by itself necessary result in meaningful privacy protection. On the other hand, in the AIC's experience, an inflexible and rigid interpretation of consent risks leading to an excessive and unnecessary

collection of data by service providers in order to be able to prove compliance with the applicable evidentiary requirements within the broader framework.

The AIC submits that a modern privacy framework should contemplate and encourage alternatives to express consent in a way which would foster the necessary protection of individuals and the innovative services and tools that they want to access. AIC members are focused on consumer privacy and each have policies and programs in place to provide transparency and informed choice to ensure that users have the opportunity to truly understand how their information is being collected and used.

By adopting compliance programs and providing transparent, easily accessible and intelligible information, the AIC believes some important results can be achieved including: (i) that data subjects can enjoy opportunities, services or other benefits, without being subject to the alternative of either giving express consent or abandoning the transaction; (ii) data subjects can be well aware of the consequences of processing as well as of their possible means of objection; and (iii) data subject will no longer be frustrated by the usual, disruptive practice of "please sign here for privacy".

The AIC requests that the Conference Committee adopt the existing drafting of Section 3(b) as provided in the Senate version of the Bill, namely:

> **"(b) Consent of the data subject refers to any freely given specific and informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent may be express or implied and evidenced by written, electronic or recorded means. It may also be given of behalf of the data subject by an agent specifically authorized by the data subject to do so."**

The AIC would also like to submit the above comments in relation to the deletion of **"EXPRESS OR IMPLIED"** from SEC. 10(a).

g.) Personal information – The AIC had earlier commented on the definition of personal information and would like to further provide comment in relation to two aspects of the definition. Firstly, clarification is sought about the intention of the inclusion of the wording: **"in a material form or not"**. If the intention is to capture both physical and electronic records the AIC believes that some ambiguity could be avoided by deleting **"in a material form or not"** and replacing with **"in a physical or electronic form"**.

Secondly, to ensure certainty for personal information controllers, the AIC proposes the further refinement to the definition of personal information: delete the phrase **"or when put together with other information would directly and certainly identify an individual"** and replace with **"alone, or in combination with other information, identifies with certainty an individual"**.

The basis for this amendment is to cover circumstances where the same piece of information can be personal in the hands of a certain data controller and functionally anonymous in the hands of another. If a specific identification, while possible, is not a significantly probable event, this information should not fall under the scope of the definition. For instance, license plates in the possession of an insurance company can reasonably be considered as "personal information," where that license plate is registered on file with other identifying information. This same information, when

contained in the tape of a security camera of a gas station, will require considerable extra efforts in order to get to identify an individual.

So too is this the case with online identifiers. An IP address is used as a basic piece of technology to enable websites to return information back to users' computers. IP addresses are issued by telecommunications providers, who have a record of the account holder, and personal information attached to that record. We might consider IP addresses in the hands of the ISP (Telco), then, a form of personal information, whereas in the hands of an online service provider, which does not have access to ISP records, they would merely be a unique anonymous identifier.

A definition that would categorize as "personal" any type of information, regardless of the possibility of that information being able to single out an individual or not will put data controllers in the position of seeing existing business procedures undermined (and having to invest resources in applying measures designed for personal data to so many other types of information). This could quickly become a competitive disadvantage in relation to more balanced regimes and severely hamper not only the ability of established companies to innovate, but also impacts the environment necessary for startups and new ideas to flourish.

We ask the Conference Committee to adopt the following definition so that a norm may be created which is clear and certain for individuals and data controllers alike while durable enough to survive the ever changing technological environment.

> **"(g) Personal information refers to any information whether in a physical or electronic form, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information alone, or in combination with other information, identifies with certainty an individual."**

h.) **Personal Information controller.** The AIC proposes the exclusion of intermediary service providers from the definition of "personal information controller." An intermediary service provider refers to an organization that brings together or facilitates transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third-parties. Excluding intermediary service providers ensures that online platforms would be appropriately protected from third-party liability, and creates the legal certainty that is necessary to allow technological innovation. It is not a new a concept and has been, in fact, implemented in Sec. 30 of the E-Commerce Act of 2000 (Republic Act. 8792) with respect to liability of service providers relating to electronic transactions. Intermediary liability protection is fundamental to the viability of the Internet as it exists today. As privacy frameworks are created or revised, robust protections for intermediaries must be a top priority.

SEC. 6 – Extraterritorial Application

The AIC submits that the practical operation of Section 6 will be to create such uncertainty due to the real possibility of a conflict of laws that it should be deleted from the Bill in its entirety.

In the experience of AIC members it is the scope and applicability of a legal privacy framework which is a critical factor in determining its success. Accordingly the AIC's preference is for the development of a clear and transparent privacy regime that does not entail extraterritorial applicability.

It is the view of AIC members that jurisdiction should not necessarily nor automatically be determined by the user's or the equipment's location. A privacy framework which ignores basic international law principles and treaties and proclaims a form of extraterritorial applicability may result in an irresolvable conflict of laws, especially for multinational corporations.

SEC. 7 – Functions of the National Privacy Commissioner

(g) AIC members request the inclusion of language which would establish some basic stakeholder consultation opportunities and transparency in relation to the creation of compliance guides developed from time to time by the National Privacy Commissioner (NPC). We submit that useful additions to this provision might include:

- require that the NPC publicize that a draft guide has been released for submissions and solicit submissions from relevant industry;
- allow submissions to be lodged by a convenient mechanism, such as internet lodgment;
- allow for a 60 day consultation/comment period; and
- as regards SEC. 7 (g) and (j) require that any NPC guide or privacy code voluntarily adhered to by a personal information controller which has been reviewed and approved by the NPC when lodged for registration is accompanied by a document that fairly summarizes the range, nature and content of written submissions received or includes all relevant written submissions.

SEC. 11 – General Data Privacy Principles

AIC members are concerned that the General Data Privacy Principles preclude many secondary purposes which are beyond the delivery of the immediate service to the user but may be reasonable and necessary in order to improve the service offered overall. Restricting the processing of personal information to only business purposes so declared prevents the flexibility of use required to drive innovation and may stifle innovation.

The AIC requests that an overarching principle is added to Section 11 which clarifies that if there is no harm caused by the processing of collected data and the data subject has the ability to opt out, the processing should be considered to be in accordance with the General Data Privacy Principles.

For example, at the end of Sec.11 insert:

> **"The processing of Personal Information for non-specified operational purposes will be considered to be within the scope of the usual and**

legitimate business practice of the personal information controller and in accordance with this Section if there is no harm caused by the processing and the data subject has the ability to opt-out."

SEC. 17 – Transmissibility of Rights of the Data Subject

It is generally accepted in law that deceased persons have no privacy interests. The underlying common law principle is much the same as in the law of defamation, which in most jurisdictions does not countenance civil actions that seek to vindicate the reputation of the dead.

Similarly the United Nations International Covenant on Civil and Political Rights (ICCPR) as well as the Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the OECD Guidelines) are not expressed to apply to deceased individuals and provide a firm indication of the inapplicability of deceased individuals within a privacy regime.

Although information about the deceased is not and should not be considered personal information, AIC members are respectful of the sensitivities of heirs and assigns under their ordinary business practices. In light of the above, the AIC requests that Section 17 is removed from the Bill in its entirety.

SEC. 18 – Right to Data Portability

Section 18 includes the following drafting: **"THE COMMISSION MAY SPECIFY THE ELECTRONIC FORMAT REFERRED TO ABOVE, AS WELL AS THE TECHNICAL STANDARDS, MODALITIES AND PROCEDURES FOR THEIR TRANSFER"**.

The AIC requests that the above phrase is deleted from this section. In our view, both the law and the Commission should remain technologically neutral. The deletion of the relevant phrase will not impact a data subject's ability to obtain data in a useable format as the remaining wording still requires that the requested personal information is to be provided by the controller in "an electronic or structured format, which is commonly used and allows for further use by the data subject".

Chapter VIII – Penalties

AIC members are extremely concerned by the severity of the custodial and financial penalties imposed under Chapter VIII. As currently drafted, the Bill provides that all privacy breaches, regardless of severity, are punishable by between 1 and 6 years imprisonment and a fine of up to Php 5,000,000. Of equal concern is that each of the penalty sections is extremely broadly defined.

Members are particularly concerned that under the current drafting of the relevant Chapter VIII sections, imprisonment is mandatory. The AIC strongly submits that judicial discretion regarding the appropriate sentencing should be introduced in each of the

penalty sections by deleting **"shall be penalized by"** and replacing with **"may be penalized by"**.

The severity of the sanctions is distinctly out of step with comparable jurisdictions and in practice will operate as a massive disincentive for investment and innovation potentially destroying growth in the local digital economy.

The AIC would appreciate the opportunity to work with the Conference Committee in order to introduce a penalty chapter which encourages compliance without stifling progress.

SEC. 34 – Extent of Liability

AIC members are concerned that the drafting of Section 34 appears to extend criminal sanctions to the responsible officers of a company and that these penalty sanctions will automatically be imposed.

The AIC submits that corporate officer liability should be limited only to those persons who had active participation in or actual knowledge of the criminal act and that an option for the exercise of judicial discretion is added to the relevant Section.

The AIC proposes the following drafting to give effect to this position:

> **SEC. 34. *Extent of Liability.* – If the offender is a corporation, partnership or any judicial person, the penalty may be imposed upon the responsible officers, as the case may be, who actively participated in, or had actual knowledge of the commission of the crime.**

Yours sincerely,

John Ure
Executive Director
Asia Internet Coalition

24 July 2012