Vincent Ma
Director, Regulatory Affairs, North Asia & South East Asia
AT&T Asia/Pacific Group Holding Ltd.
30/F, Shell Tower, Times Square
1 Matheson St.
Causeway Bay
Hong Kong

T: +852 2506 5544
F: +852 2506 0308
E: vincent.ma@ap.att.com

By Email (MICA_DP_Public Consultation@mica.gov.sg)

October 25, 2011

Comments of AT&T on the Consultation Paper on the Proposed Consumer Data Protection Regime for Singapore

AT&T Worldwide Telecommunications Services Singapore Pte Ltd. ("AT&T") respectfully submits these comments on the Consultation Paper on the Proposed Consumer Data Protection Regime for Singapore issued by the Ministry of Information, Communications and the Arts of Singapore ("the Ministry"), published on 13 September 2011 (the "Consultation Paper").

Operating globally under the AT&T brand, AT&T's parent, AT&T Inc., through its affiliates, is a worldwide provider of Internet Protocol (IP)-based communications services to businesses and a leading U.S. provider of wireless, high speed Internet access, local and long distance voice, and directory publishing and advertising services, and a growing provider of IPTV entertainment offerings. AT&T Inc. operates one of the world's most advanced global networks, carrying more than 18.7 petabytes of data traffic on an average business day, the equivalent of a 3.1 megabyte music download for every man, woman and child on the planet. With operations in countries that cover 97% of the world's economy, AT&T Inc. has extensive experience as an incumbent and a new entrant, as a fixed line operator and a mobile operator, and in the dynamic areas of converged technologies and services.

In Singapore and other Asia Pacific countries, AT&T Inc., through its affiliates, is a competitive provider of business connectivity and managed network services and is a leading provider of bilateral connectivity services linking the U.S. with Singapore and all other Asia Pacific countries.

AT&T appreciates the opportunity to express its views in this public consultation on the proposed consumer Data Protection regime and hopes that its comments will be helpful to the Ministry in developing policies that both protect consumer privacy and nurture the investment and innovation necessary for the sustainable development of the Information Society within Singapore, and between Singapore and the globally interconnected Internet networks. To maintain the pace of innovation on the Internet, both governments and the private sector must continue to find ways to strengthen consumer trust online, which will, in turn, increase Internet usage and adoption both domestically and internationally.

The Need for a Flexible Approach to Data Protection Regulation: It is essential for governments and regulators to strike the right balance between data protection and innovation in technology and business models. To facilitate the continued development of the global Internet, as well as other critical cross-border network services, data protection

rules should be flexible and simple enough to encourage the development and take up of innovative new services. Cross-border network services, including the Internet, have contributed substantially over the recent decades to national and global productivity, efficiency, network resilience and prosperity. Newly evolving cloud computing services also represent tremendous opportunities for public benefit as their availability becomes more widespread. While many cloud products are similar to the hosting, network-based computing and virtual private network managed services that have been available for years, recent technologies now make it possible to achieve significant efficiencies, and to offer services on a more flexible, usage-based model, which can be even more affordable and resilient.

Notwithstanding the generally supportive policy environment for cross-border data services in most countries, there are some policy areas with the potential to create systemic risk to the further development of these services, including data privacy requirements that due to their scope, inconsistency and uncertainty, may limit cross-border data flows more broadly than required.[1] To avoid these potential harms, AT&T believes that governments should establish flexible policy frameworks for data privacy that encourage self-regulatory initiatives – such as the forward-looking privacy policy encouraging user control over information described below – that are better-suited to this fast-changing marketplace than traditional regulatory approaches. In particular, the role of governments should be to advocate on behalf of transparency, clarity and flexibility, while also ensuring that privacy-by-design initiatives neither prescriptively mandate nor prohibit any particular feature or system configuration, which could hamper innovation. Policymakers should promote privacy-by-design principles through a proactive and cooperative approach and should avoid setting unduly prescriptive standards that may impede the development of the new innovative services and uses of information that consumers' desire.

A flexible approach to regulation can play an important role in ensuring strong privacy protections, particularly as data is now routinely moving across jurisdictional boundaries, thereby complicating regulatory efforts by national authorities. To this end, governments should engage with industry and other stakeholders to encourage the development of flexible accountability mechanisms like industry codes of conduct or other codes of practice. Similarly, approved non-governmental certification agents may be used to help oversee privacy practices and provide greater accountability and consistency among service providers. Under this approach, data protection authorities would still maintain their

[1] Other significant potential risks to the further development of cross-border services include: local infrastructure requirements that mandate placing certain servers or hosting capabilities within a jurisdiction as a condition of serving customers there; law enforcement assistance requirements that are applied in manner that is not narrowly tailored and proportionate; and network security standards that are established on a national basis and not consistent with widely accepted international best practice standards for network security.

oversight and enforcement authority.[2] Such an approach would allow for improved efficiencies and would be much better suited to the fast-changing Internet and cloud computing markets than traditional regulation.

Privacy Policy Should Encourage User Control Over Information: AT&T believes that a policy framework which protects consumer privacy and engenders consumer trust is the foundation for promoting continued innovation and the free flow of information on the Internet. The changing Internet marketplace requires a model of privacy protection that moves beyond notice and consent and toward customer engagement and control. Privacy should not be a "back-end" compliance consideration, but rather must be a foundational value under a "privacy-by-design" approach. Privacy policy frameworks should be fundamentally rooted in the consumer's interest in controlling the integrity, use and dissemination of his or her identity in the online world. In turn, this consumer control focus will strengthen the trust environment on the Internet, which is essential to unlocking its potential social, economic and cultural benefits.

Enabling user control over information as a means to building trust should guide policy making by all actors in the Internet ecosystem, including both public and private sector entities. For AT&T, such an approach means we are committed to integrating privacy as a feature into AT&T's product design and various business models, and building capabilities for our customers to understand how information is used and to exercise meaningful control over their privacy.

The Internet holds the promise of stimulating historic progress, not only in economic and technological development, but also in the health care and financial sectors, energy independence, education, social connectivity and cultural production, and other areas. This promise is inextricably linked to a foundation of user trust in both the public and private sector online entities with which users interact as well as in the safety and security of the Internet itself. Just as in the physical world, Internet users should have meaningful control over their transactional experiences. An online privacy paradigm that emphasizes user control will strengthen the foundational trust environment of the Internet.

A focus on consumer engagement and meaningful user control provides the critical foundation for promoting a trust environment. The means for effective consumer engagement must be designed as an integral attribute of the online experience, providing demonstrable value to the customer. For example, consumers will be better served if there is transparency and choice regarding the collection and use of their information at the time it is collected and used.[3] Consumers may decide to make their personal information available

[2] However, any data breach liability or other legal remedies should be based on evidence of actual economic harm.

[3] This does not mean that one privacy regime will be immediately supplanted by an entirely new one, as the use of straightforward and meaningful notice-and-consent systems can and

where they see the value of doing so and are confident about their ability to control its use. Moreover, Internet users clearly understand and accept that information will be collected in commercial relationships, and that the information will be used to offer goods and services that are of value to them. But as a general industry matter, consumers need more information about what data are collected, how personal information is used and shared, and how it is protected.

Innovative approaches to engaging consumers through increased transparency and control tools that have begun to emerge in the marketplace can serve as a model for the next phase in the evolution of privacy practices. AT&T sees that model as shifting the current focus from merely notifying consumers of data collection towards facilitating practices that promote the creation of value for consumers. This model would focus on ensuring that data practices are fully transparent (as opposed to merely disclosed) and that customers are engaged and have the opportunity to control their privacy and the use of their personal information.

The further development of privacy-enhancing technologies to improve transparency and give consumers greater control over personal data therefore should be encouraged. With improved tools, consumers will be better-positioned to make informed choices about protecting their own privacy. For example, anonymized browsing helps prevent the hidden or unknown collection of a user's data through data collection mechanisms, such as cookies. In addition, consumer-centric identity management systems could include the ability to allow users to build virtual profiles that support their information sharing choices online across various websites, applications, and platforms. Using these systems, consumers could actively manage how they will exchange personal information in pre-determined ways. Improved and ubiquitous identity management solutions could help individuals and organizations form trusted communities based on varying degrees of identity exposure. Through a virtual profile, a user could have the option of identifying the level of information he or she wishes to share with different communities, including trusted businesses, friends, or even no one. Such systems could also allow users to establish notifications that alert them before certain information is shared and to track generally when and with whom their personal data is shared.

Data Protection and Business-to-Business Services: It should be recognized that the data protection concerns and interests of multi-national corporations (MNCs) and other large business customers in connection with the purchase of Internet and other data services differ significantly from those of individual consumer customers. In the large business market, customers are generally sophisticated and services are highly complex, often involving a customised and dynamic mixture of infrastructure, platform and software services delivered on the widest scale to geographically spread businesses with a guaranteed

---

will be appropriate in a variety of circumstances. However, more interactive forms of customer engagement should be part of the evolution of privacy practices.

quality of service. These extensively negotiated commercial arrangements are normally set forth in Service Level Agreements (SLAs) or End User Agreements, and involve negotiations by highly sophisticated parties and legal counsel. An extensive regulatory overlay to this market-based model is both unnecessary and potentially harmful.

Business-to-business services service contracts typically establish roles and responsibilities of the parties with regard to the fulfillment of data protection requirements, as well as the agreed-upon jurisdiction for contract governance. Any data protection requirements applicable to business-to-business service arrangements should be sufficiently flexible to allow the parties to reach agreement on the assignment of responsibility for such requirements. Regulators should avoid undermining the certainty provided by contractual agreements that establish consistent provisions and processes that can be relied upon by the parties across jurisdictions. Regulators also should avoid establishing overly detailed and divergent privacy and other regulatory requirements that cannot be accommodated in a unified service level agreement between the service provider and the business customer. When business customers have agreed to the roles of each party relative to data protection and the governing law, and there is a reasonable nexus to the subject of the contract and the agreed law, this contracted preference should prevail.

Attempting to standardise SLAs with regard to data protection requirements would risk stifling competition in the provision of services to these customers, which relies precisely on the different performance and service levels that the various providers can offer. Any levelling of these arrangements would harm both users and providers, by reducing customers' choices for trade-offs among factors including price and quality, and undermining providers' competitiveness.

The Need to Encourage Global Interoperability: The Consultation Paper properly notes the need to ensure consistency with international standards, such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the APEC Privacy Framework ("APEC Framework"). This approach promotes a consistent global approach to privacy protection to avoid the creation of unnecessary barriers to information flows and to remove impediments to trade. In addressing international issues, an important objective is giving providers technical and operational flexibility so that services can be designed to meet the needs of customers, rather than overly restrictive legal and regulatory requirements.

Governments also should work towards mutual recognition of privacy standards with other countries and regions to avoid any impediments to the cross-border data flows that are critical to the global growth of many services, including cloud services. Such an approach can play a leading role in establishing a flexible policy framework that reflects fast-changing technical and market developments, while also facilitating greater consumer privacy cooperation across country borders. There is broad consensus on the most important privacy and security principles that can form the basis for a global framework that is better designed

at&t

to promote cross-border data transfers. [4] In particular, the APEC Framework, which was recently adopted by the Electronic Commerce Steering Group, sets forth a broadly-applicable privacy standard that can be adapted to particular jurisdictions and industries while enjoying mutual recognition by participating economies. AT&T therefore recommends that the Ministry should provide a flexible framework that allows compliance with international frameworks such as the APEC Framework to function as a "safe harbor" for compliance with any data protection requirements that are adopted here.

* * *

AT&T would be pleased to answer any questions concerning these comments.

Respectfully submitted,

[Vincent Ma]
for AT&T Worldwide Telecommunications Services Singapore Private Limited

[4] For example, the OECD recently convened a high-level meeting on the Internet economy, which produced a set of principles for Internet policy-making agreed to by Member States, the Business and Industry Advisory Committee and the Internet Technical Community. *See Communique on Principles for Internet Policy-Making*. The principles include strengthening consistency and effectiveness in privacy protection at a global level.