Report on Cloud Data Regulations

A contribution on how to reduce the compliancy costs of Cross-Border Data Transfers

A joint report by
The Asia Pacific Carriers' Coalition (APCC) and
The Asia Cloud Computing Association (ACCA)

APCC
asia pacific carriers' coalition

asia cloud computing association

Report on Cloud Data Regulations: A contribution on how to reduce the compliancy costs of Cross-Border Data Transfers

Contents

Cloud Data Regulations

A contribution on how to reduce the compliancy costs of Cross-Border Data Transfers

> "States have made relatively little progress to identify an acceptable solution to cross-border transactions involving personal data. It is, admittedly a very difficult issue that has not become easier to address over time but is rather becoming more acute in light of the growing importance of data processing in the global economy." (*Cross Border Data Flows and the Protection of Privacy*, Hague Conference on Private International Law, 2010, p.7)[1]

A: INTRODUCTION

The purpose of this paper is to contribute to, and help drive the formation of, policies concerning cloud computing in Asia. The paper addresses the increasing complexities surrounding the transfer of data between jurisdictions, and the problems this poses for operators, such as carriers, remittance service providers, social networks, Internet and e-commerce companies, offering legitimate cross-border data transfer services. As the opening citation suggests, progress towards a harmonized solution has been slow, but the urgency to find one has increased.[2]

This paper, commissioned by the APCC, builds on original research developed by the ACCA as part of a broader and ongoing study on Data Sovereignty throughout the Asia Pacific. It argues that law makers and regulators should balance their efforts to protect personal data privacy and data in key sectors, such as banking and health services, with solutions that facilitate and therefore lower the cost of data transfers under all reasonable circumstances.

Finding the right balance between data safety and data access requires, almost by definition, a multi-stakeholder approach. Finding a balance is important if the full benefits of international trade in goods, services and e-commerce are to be realised by reducing unnecessary costs of doing business. While the frequency of cross-border data transfers are increasing with the proliferation of cloud computing usage, the costs of compliance are significant and growing. For example, an increasing number of jurisdictions require a company to appoint a data protection officer (see Table 1 below). Every jurisdiction has its own approach and, within each jurisdiction, there may be general laws, sector-specific laws, different sets of regulators, different ways to apply the laws and, in some instances, different case law decisions of the courts that interpret those laws.

The paper is divided into the following sections.

- The link between cross-border data transfers and the growth of international trade in goods, services and e-commerce.
- The growing use of cloud computing and the implications for cross-border data transfers.

[1] Hague Conference on Private International Law, March 2010, Cross-Border Data Flows and Protection of Privacy. http://www.hcch.net/upload/wop/genaff2010pd13e.pdf

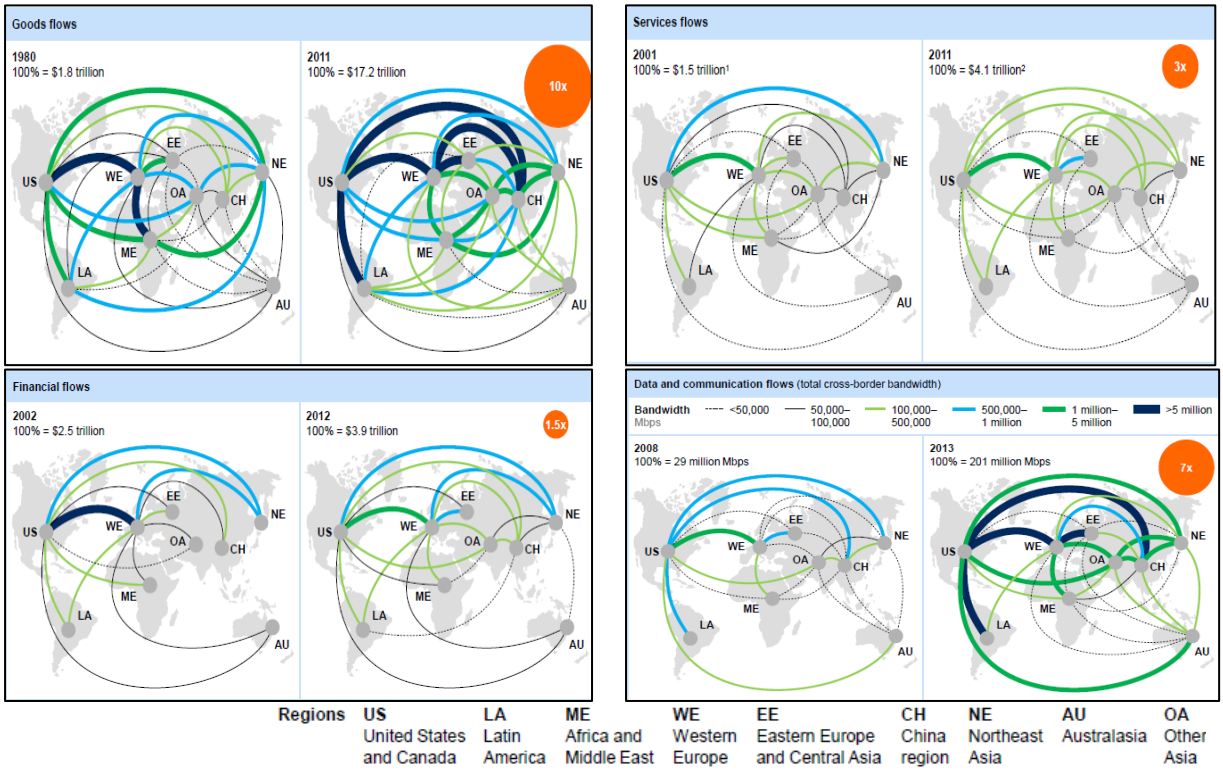
[2] "As early as 1981, the Explanatory Memorandum to the OECD Guidelines contemplated such an approach but recognised that a solution based more on private international law would be very difficult." (p.7)

- The growing complexity of laws and regulations governing cross-border data transfers and the needs of compliance.
- Ways forward to harmonize and fast-track cross-border data transfer regulations: striking the balance
- Conclusions and Recommendations

B: Cross-Border Data Transfers and International Trade

Cross-border trade in goods, services and e-commerce, and the data flows that underpin them, are fundamental to modern and developing economies. As the following graphs from McKinsey & Company illustrate, the global growth of total bandwidth for communications from 1980 to 2011 was x7 to support trade growth in the value of goods (x10), in the value of non-financial services (x3) and in the value of financial services (x 1.5).

Graphics 1-4: Growth of World Trade in Goods, Services, Financial Flows, and International Bandwidth in Data and Communication Flows

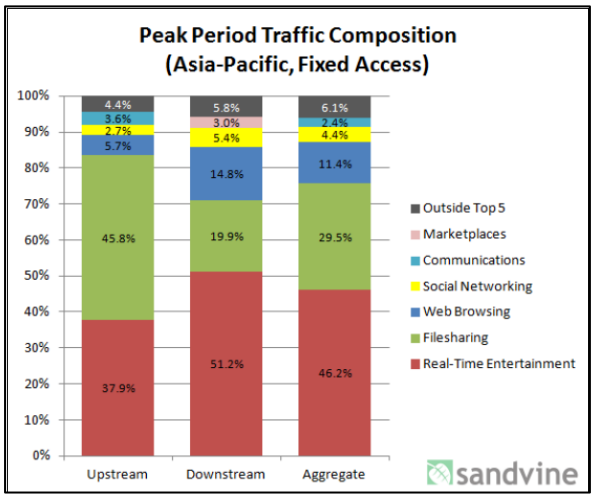


Source: McKinsey, April 2014, Global Flows in a Digital Age http://www.mckinsey.com/insights/globalization/global_flows_in_a_digital_age

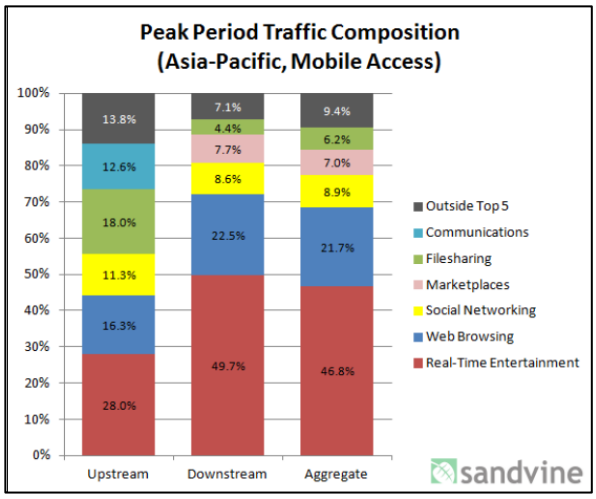
The figures in Graphics 1-4 show the global value of all goods, both physical and digital. Graphic 5 (below) selects only digital trade or e-commerce. Drawing a direct *proportional* link between data flows and trade is not advised as there are methodological issues when selecting the relevant metrics. First, not all data traffic is directly, or even indirectly, related to trade, for example, online "chat" and file-sharing on social media may not be. Indeed while "file sharing" is an important productive component of private business and commerce and a method of collaborative working that boosts productivity, in terms of volume it relates primarily to P2P video-sharing of movies and music videos

which generates substantial traffic uploading as well as downloading, especially in Asia.[3] Therefore attempts to correlate data flows *exactly* to e-commerce will be frustrated, skewed, by the growing 'weight' of video in the total volume of cross-border traffic.[4,5] Graphics 5 and 6 from the Sandvine *1H 2013 Global Internet Phenomena Report* covering the regions of Asia-Pacific, Europe, Latin America and North America, show the overwhelming proportions of traffic over fixed lines and mobile that is accounted for by "entertainment" and "file sharing".

Graphic 5



Graphic 6



Source: Sandvine, 2013, Global Internet Phenomena Report https://www.sandvine.com/downloads/general/global-internet-phenomena/2013/sandvine-global-internet-phenomena-report-1h-2013.pdf

Second, the data available for consumer use of the Internet through audits of ISPs and social networks, is more immediately available than in the enterprise and state sectors where a high proportion of the traffic passes through private networks or over networks managed by carriers and other service providers.[6]

Despite these and other concerns – for example, there is a substantial proportion of international dark fibre which, if included in the bandwidth data, would exaggerate capacity linked to trade – the use of the growth in bandwidth capacity can be a useful 'approximate illustration' of the important relationship between data flows and the growth in trade in goods and services in the digital global economy.

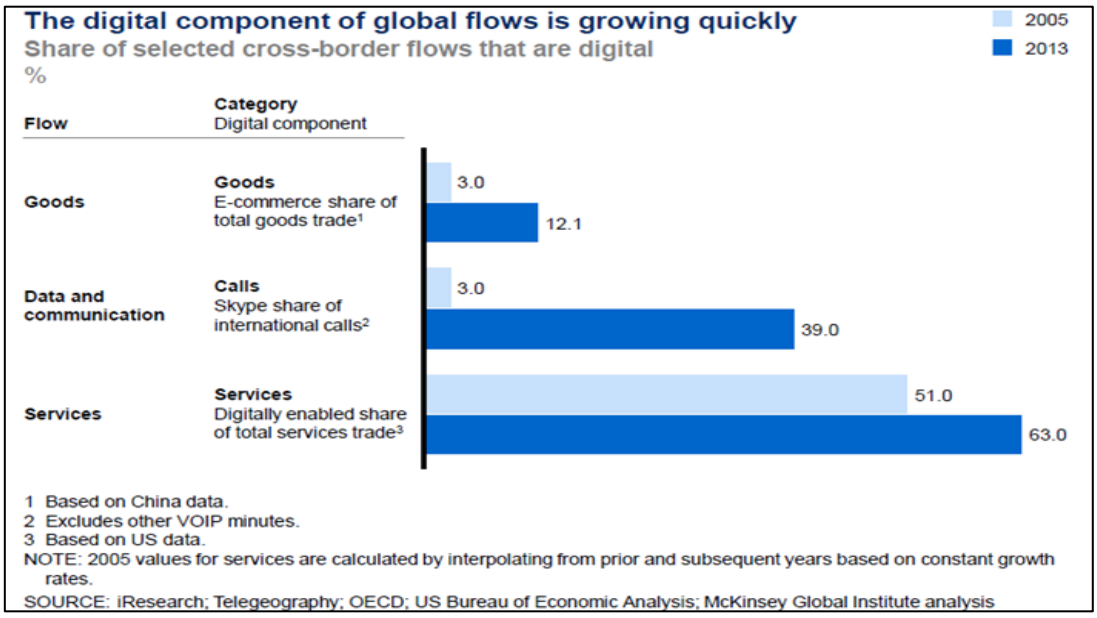
[3] See Sandvine (2013) Global Internet Phenomena Report **https://www.sandvine.com/downloads/general/global-internet-phenomena/2013/sandvine-global-internet-phenomena-report-1h-2013.pdf**

[4] To clarify this point, the downloading of "pirated" video *will not* be registered as e-commerce, but the demand for P2P downloads *will* register as a demand for bandwidth which is sold by telecom companies. So the growth in bandwidth will reflect the growth in data traffic, albeit not in a 1:1 ratio, but not, in this case, in the same ratio as it reflects the growth in trade in services and e-commerce. The issue is also discussed in Box 4.1 http://www.usitc.gov/publications/332/pub4415.pdf.

[5] Although currently most P2P video sharing is unpaid, for the future enterprising start-ups may well find a way to monetize this market, just as companies like Spotify have done with "free" music downloads.

[6] For this reason, Cisco's forecasts of Internet traffic growth, which include estimates of private sector data flows, are typically higher than others. It is therefore important to know the methodology before comparing forecasts.

Graphic 7



Source: McKinsey, April 2014, Global Flows in a Digital Age http://www.mckinsey.com/insights/globalization/global_flows_in_a_digital_age

From the above it is clear that law makers and regulators need to view cross-border data flows as an essential component and facilitator of trade in goods, services and e-commerce.

C: Cloud Computing, Data Centres and Data Transfers

A modern trend in IT is towards cloud computing. Although there are many competing definitions of the term,[7] there are three important elements. First, technically it means the ability to store, process and retrieve data and software in the Internet cloud. Large enterprise corporations and governments started to build their own private cloud networks supplied by companies such as Cisco, EMC, IBM, Microsoft. Email from Hotmail in the late 1990s[8] and from Gmail in 2004 were the first public applications.

Second, from a business perspective, it offers a way to rent software, data storage, computing power at a distance rather than buy or lease software and memory capacity on the hard disk of a personal computer. This has given rise to public cloud services in parallel to in-house private clouds and to hybrids. Hybrids arise when some of the less mission critical business operations and data are out-sourced to a public cloud service provider, or when capacity in the public cloud is used to supplement computing power in the private cloud, for example, at times of peak demand. Amazon Web Services (AWS) are a good example of offering such a service.

Third, from a communications perspective, cloud computing offers an efficient way to transfer data from one location to another to facilitate global collaborative working, cross-border supply chain

[7] OECD (2009) "In 2008 the term 'cloud computing' became fashionable as a way to refer to a number of interlinked information technology trends. There are a number of competing interpretations of what cloud computing is about, but in its simplest formulation the expression refers to the provision of computing resources at a distance, over the Internet." *ICCP Technology Foresight Forum - "Cloud Computing: The Next Computing Paradigm?"* http://www.oecd.org/internet/ieconomy/iccptechnologyforesightforum-cloudcomputingthenextcomputingparadigm.htm.

[8] Hotmail began in 1996. Microsoft acquired it in 1997.

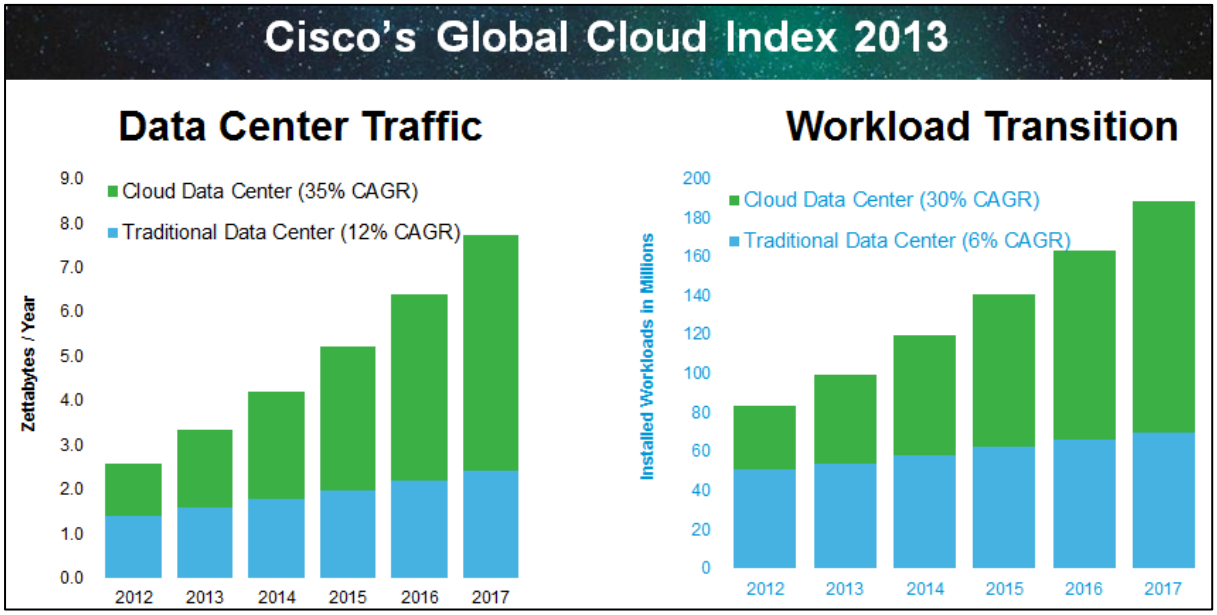
management and to support e-commerce, and trade in goods and services. In this sense, cloud computing is a technology that adapts perfectly to the growth of a globally interconnected economy.

Although the early adopters have been the world's leading international companies, cloud computing offers an opportunity for business of all sizes in developing economies to enter world markets at lower cost and with greater reach. This is because of savings in the IT budget for equipment, software and skilled personnel, and because the cloud offers close to zero-cost to connect with partners, suppliers and customers overseas.

Data Centres

Data centres, which have long been available for data storage and retrieval, are now an essential part of the supporting infrastructure for cloud computing, along with broadband connectivity. Early data centres were little more that containers fitting with a racks of servers and air conditioning units. Today data centres can be server farms on a massive scale. As of 2013, Amazon had around 450,000 servers concentrated in 7 data centres located in different parts of the world. Google has an estimated 900,000 servers located in 15 data centres.[9] Facebook's new Princeville server farm covers 62,000 square feet, but as early as 1989 Microsoft's first data centre covered 89,000 square feet. Microsoft is estimated to have spent well over USD20 billion on data centres. By 2013, Facebook was processing around 750TB of data per day. The scale of data centres and their processing power, together with their electricity consumption,[10] is truly staggering and growing all the time.[11] Cisco forecasts that cloud data centric workloads will overtake those of traditional data centres within the next 1-2 years (Graphic 8).

Graphic 8:Traditional vs. Cloud Data Centre workload distribution,2011-2017 Forecast



Source: Cisco Global Cloud Index 2013, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html

[9] Google added data centres in Singapore and Taiwan in 2014 to its 13 data centres listed in 2013.
[10] A large data centre consumes as much electricity as a small town. The largest data centre in the USA has 53 generators and uses 8.5 million gallons of cooling fluid a year. Modern server farms try to make use of solar and hydro-electric power and even Artic ice conditions.
[11] See http://storageservers.wordpress.com/2013/07/17/facts-and-stats-of-worlds-largest-data-centers/

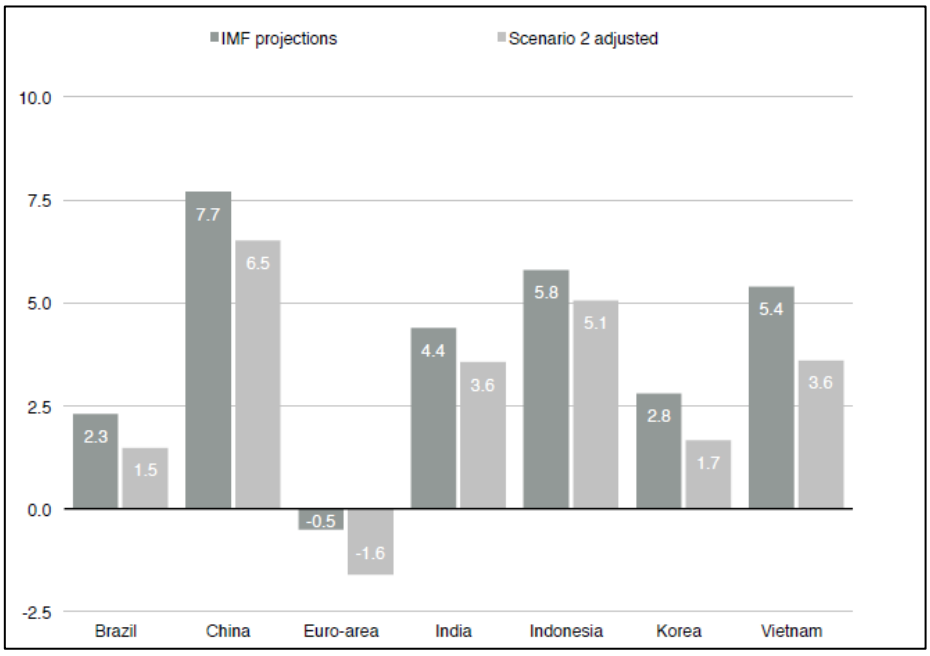
Data and Data Centre Localization

Data centre 'localization' issues arise when governments stipulate that foreign companies offering Internet-related services, such as e-commerce or social networks or cloud computing services, not only keep certain categories of data 'local' by not transferring it out of the country, but require them to invest in a local data centre where the data can be stored, and could be available for local inspection.

The economic argument *for localization* is to encourage the growth of domestic cloud service providers, possibly as majority partners in joint ventures with foreign service providers. This is an entirely separate argument from the view that keeping data local will keep it more secure, a view that relies heavily upon the unlikely assumption that local defenses against cyber-hacking are more stringent than in other jurisdictions, that power supplies are plentiful and uninterrupted and environmental such as earthquakes are unlikely.

The economic argument *against localization* of data is determined primarily by the scale of localization. For example, the European Centre for International Political Economy (ECIPE) modelled the impact of across-the-board, as opposed to sector-specific, localization of data and compared the projected GDP growth rates with those forecast by the IMF for 2014. Graphic 9 shows the outcome of the hypothetical case. In the short run it is detrimental to growth; for example, Indonesia's projected GDP growth rate would come down by 0.7 per cent and in Vietnam by 1.8 per cent.

Graphic 9: IMF Projected GDP growth (2014) adjusted for Across-the-board **localization** , c**hanges in %**



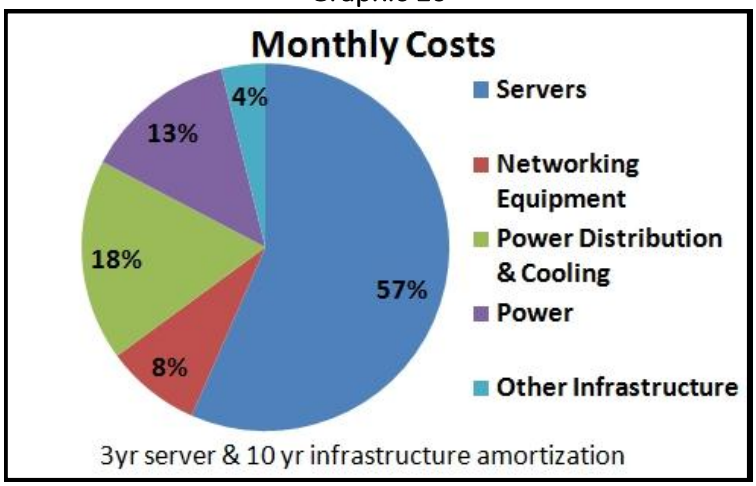
Source: European Centre for International Political Economy (ECIPE), April 2014, The Costs of Data Localisation: Friendly Fire on Economic Recovery http://www.ecipe.org/media/publication_pdfs/OP0314.pdf

Most international companies will find problems with such a requirement, and given that companies based in the Asia-Pacific region tend to be smaller than their multinational cousins, even more so. The challenges include the cost of building and operating a data centre, downtime when energy supplies

or other inputs are disrupted so the service falls far short of the 'Five Nines",[12] as well as security which may be difficult to guarantee in locations where security issues are a more general problem.[13] Even building a comparatively small data centre to meet the demands of localization would entail upfront investment costs which easily reach upwards of USD50 million depending upon whether it is a Tier I, II, III, or IV facility.[14] And while the cost of equipment is falling, energy costs are less predictable and more crucially, energy supplies maybe less predictable. In the US, estimates suggest data centres consume more than 2% of total energy supplied – and the proportion is rising.[15] A big question mark for developing economies in Asia is: can their energy infrastructures support a big increase in demand without denying other local users?

Graphic 10 illustrates estimates of monthly data centre costs as modelled by James Hamilton. He amortizes the costs of the infrastructure over a 10 year period and the cost of servers over 3 years to normalize (annualize) the cost statistics. While the start-up costs are primarily infrastructure, over time server costs followed by the costs of power, power distribution equipment and cooling equipment costs eat up most of the annual budget.

Graphic 10



Source: Source: Perspectives: James Hamilton's Blog, 18 Sep 2010, Overall Data Center Costs, *http://perspectives.mvdirona.com/2010/09/18/OverallDataCenterCosts.aspx*

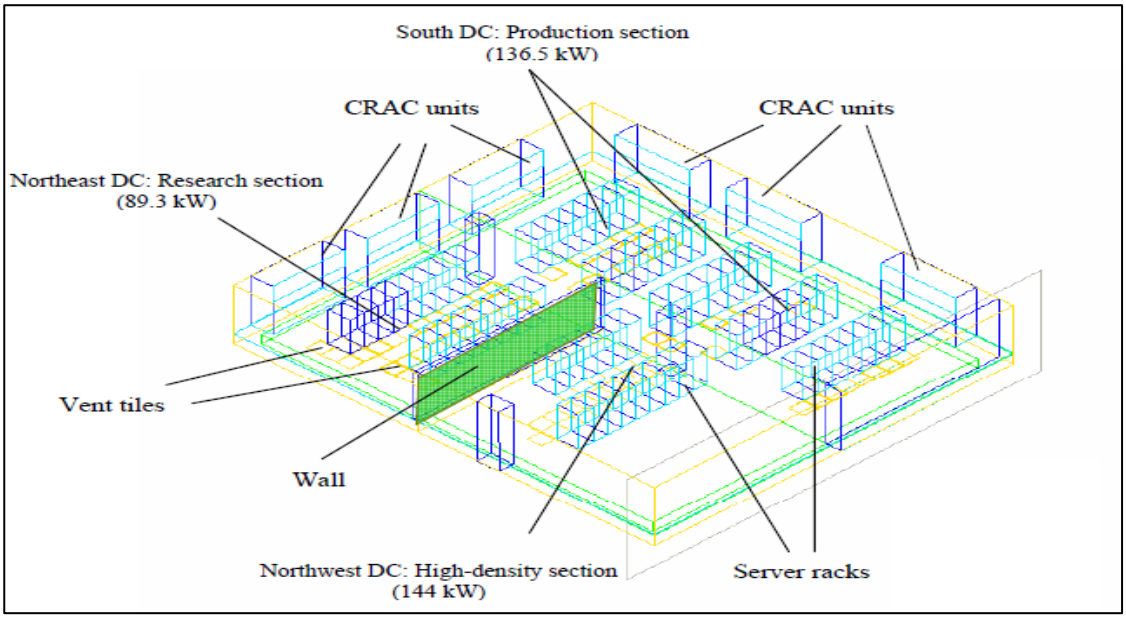
Although the costs of land and labour may be lower in most Asian developing economies than in the US or Europe or Japan, the qualitative issues are paramount where international business is concerned. The level of performance of cloud computing and the accessibility and security of the data stored in the data centre will make or break the reputation of a cloud service provider in what is an intensely competitive global market.

Graphic 11 illustrates a typical data centre architecture. There is a difference between running a traditional data centre and running a cloud data centre. Traditional data centres often cater for a greater proportion of high-end and more expensive applications that use their facilities. When these move onto the cloud they will often move into private clouds. Traditional data centres also have

[12] 99.999 % uptime as service level agreement (SLA) performance target.
[13] The ACCA's *Cloud Readiness Index 2014* lists the three economies that are imposing localization of data centres, namely China, Indonesia and Vietnam, 10th and jointly 11th out of 14 economies – for the Summary Report see http://www.asiacloudcomputing.org/images/research/ACCA_CRI2014_ExecSummary.pdf
[14] Tier 1 aims at 99.67% availability, Tier II at 99.749%, Tier III at 99.982% and Tier IV at 99.995% as documented by the Uptime Institute. For a useful summary, see http://abrconsulting.com/UptimeDoc.htm
[15] Estimates of the Energy Information Administration, see reference at http://www.treehugger.com/gadgets/designing-radically-efficient-and-profitable-data-centers.html

legacy costs to cover, such as maintaining aging applications and infrastructure. Some estimates show 80 percent of spending on maintenance.[19]

Graphic 11



Source: http://www.hpl.hp.com/techreports/2005/HPL-2005-107R1.pdf

An important distinction is that cloud data centres are not remodelled traditional data centres, but purpose built, running a more limited range of applications that imply a different, often a lighter workload pattern, and which operate across standard and therefore interoperable equipment, networks, OS, etc. Their scale can range from the massive Amazon data centres hosting on average over 60,000 servers each, to small scale 10,000 server centres, but all with lower unit costs than traditional centres.[20, 21]

Regional Cloud Service Providers

Given these costs, unless the cloud service provider has sufficient local business to scale up to a data centre investment, the decision to invest is a difficult one. Mega-investments of this kind are less of a problem for the global giants who have a global market in view, but for essentially regional data centre service providers the commercial decision is difficult.

This implies problems for service providers from developing Asian economies. The global giants are competing more and more at the service level through SLAs, and because the cloud can provide the guarantees that if the service is not available in one world location it can be made available from another, they are in a strong position to win cross-border data transfer business. They are also in a strong position to store a customer's data only in those locations where the customer agrees and to

[19] The average cost per year to operate a large data centre in the US is usually between USD10 million to USD25 million. In many Asian economies the cost would be less. See http://www.dummies.com/how-to/content/comparing-traditional-data-center-and-cloud-data-c.html

[20] Costs can be measured in different ways as can charges to the customer. The cloud data centres are trending towards an energy per-Kw-usage model. By contrast, for a per-rack space model of costs see the Uptime Institute (2007) *A Simple Model for Determining True Total Cost of Ownership for Data Centers*
http://www.missioncriticalmagazine.com/ext/resources/MC/Home/Files/PDFs/%28TUI3011B%29SimpleModelDeterminingTrueTCO.pdf

[21] According to one source, ccomputing costs as a percentage of total costs tend to be around 40% for traditional data centres and upwards of 50% for cloud data centres, as non-directly related computing costs fall in cloud centres. See http://www.dummies.com/how-to/content/comparing-traditional-data-center-and-cloud-data-c.html

avoid jurisdictions where data privacy laws are weak. That means some cross-border trade for developing economies may be impeded, so developing economies should have a self-interest in aiming for a balance between strong data protection laws and very open cross-border data transfer policies that streamline compliance to necessary safeguards. One emerging idea, discussed further below, is for data centres to quarantine certain categories of data, such as personal data, sensitive data, data coming under local sector regulations, government data, and so on. Different rules may apply to different categories and where data transfers are restricted the data can be "warehoused".

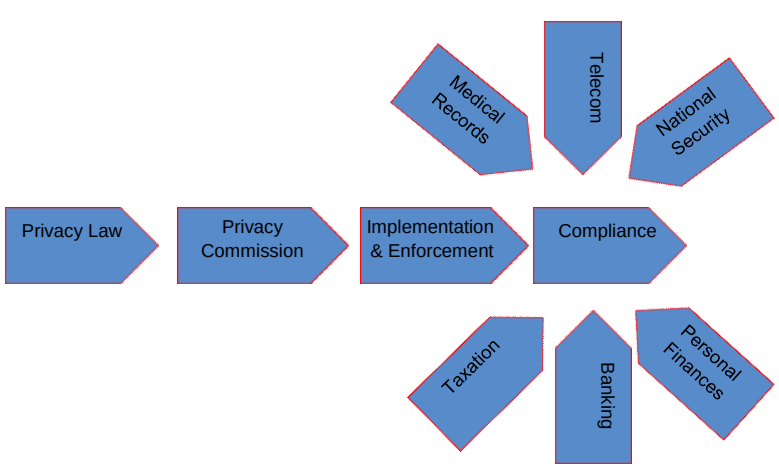
Such policies would benefit regional Asian players because then they too could offer SLAs using their cloud data centres in other locations in the Asia-Pacific to provide 99.999% uptime and full scale disaster recovery services. Otherwise, with restrictions and expensive compliance conditions in place, data centre backup from the USA and Europe will always out trump a purely Asian-based service. It is important therefore for law makers and regulators to come to a good understanding of the intricacies of the emerging data centre markets in order to achieve the right balance between data accessibility, privacy and protection.

D: Data Privacy and Protection Laws and Regulations

The core problems facing cloud service providers and others who need to transfer data across borders are how to ensure compliance with an alphabet soup of general and sector-specific laws and regulations and codes of practice and legal judgments and legal and procedural uncertainties that differ in their details across so many jurisdictions.

For example, in some cases laws exist on the statute book but are not being implemented. Because cloud computing is a relatively new development in the world of data processing and data transfer, especially in Asia Pacific, there is enormous uncertainty. The uncertainty exists at all levels, from policy makers and regulators to "data controllers" (companies and organizations) responsible for collecting, storing and processing data, to persons and entities to whom the data relates.[22] This is not a surprising situation, but for the efficiency and effectiveness of data protection and of data processing for commercial and non-commercial purposes, a level of alignment of terminologies, standardization and common practice is needed.

[22] According to the OECD, a '"data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;'
http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part3
.



The Cost of Compliance?

Inevitably, bringing common practice into the situation, and possibly fast-tracking some of the procedures, can only come about after some trial and practice, through the discovery of where real problems *do* exist as opposed to where hypothetical problems *could* exist. Keeping a watchful eye on the lessons from other jurisdictions is one way to move towards some means of harmonization to reduce the costs of doing business across the region. Tables 1 and 2 summarize the status of personal data protection laws and regulations regarding cross-border data transfers.

Table 1: Summary of Data Privacy Laws and Data Transfer Provisions

Country	General law on personal data privacy protection	Separate regulator	Register of data controller	Sector-specific regulation	"White list" countries or requirement on data controllers to ensure protection on data transfers	Individual consent required for data transfers	Contract obligations accepted as reason for data transfers	Companies required to appoint 'Data Protection Officer'
Australia	Y	Y	Y	Y	Y	Y	Y	N
New Zealand	Y	Y	N	Y	Y	Y	Y	Y
India	N	N	N	Y	Y	Y	Y	Y
Indonesia	Proposed	N	N	Y	N	Proposed	N	N
Hong Kong	Y	Y	Y/N	Y	Y/N	Y	Y	N
Japan	Y	N	N	Y	Y	Y	Y	N
Malaysia	Y	Y	Y	Y	Y	Y	Y	N
Philippines	Y/N	Y/N	N	Y	Y	Y	Y	Y
Singapore	Y	Y	N	Y	Y	Y	Y	Y
South Korea	Y	N	N	Y	Y	Y	Y	Y
Taiwan	Y	N	N	Y	Y	Y	Y	N
Thailand	Y	N	N	Y	Y	Y	Y	N
EU	Y	Y	Y	Y	Y	Y	Y	Proposed
UK	Y	Y	Y	Y	Y	Y	Y	Y
USA	N	FTC	N	Y	N	By sector	Y	Varies

Note: (i) Y/N means it is on the stature book but not yet implemented.

Of the jurisdictions listed, and apart from the USA which has a series of sector-specific laws and regulations, as of 2014 only India and Indonesia do not have a general law protecting personal data, while the law passed in the Philippines has not yet been implemented. Besides the USA, seven jurisdictions do not have a separate regulator or commission for data privacy. Besides the UK and EU which has provision for it, only Australia and Malaysia have introduced a register of data controllers.

Hong Kong has not implemented it. All have some sector-specific regulation governing data protection in areas such as telecoms, banking, health, etc., and in this regard the devil is in the details as they differ across jurisdictions and each data controller must be able to comply in each case.

Besides the USA, all have laws and regulations governing cross-border data transfers. The EU-model is "location-based", requiring the external territory to have an acceptable level of data protection. The APEC approach is "accountability-based" whereby the data controller is legally responsible for making the decision as to how far the external territory has an acceptable level of data protection. In reality, because each jurisdiction (with the current exception of Indonesia) allows cross-border data transfers under certain conditions, such as the individual giving their consent, a contractual obligation involved, it being in the best interests of the data owner, etc., the distinction between these approaches is often more apparent than real. In the USA, what has been called a "risk-based"[23] approach places the onus on each separate data controller to comply with sector-specific regulations.

Data Protection Officer

The last column of Table 1 lists five Asian jurisdictions where there is a requirement for the data controller to appoint a data protection officer (DPO) to ensure compliance. This is in addition to an obligation in most jurisdictions to ensure the security of the data collected and stored, and in some cases a requirement to publish a data privacy policy.

There is some uncertainty surrounding a requirement for a DPO. For example, the European Union is proposing all companies employing more than 250 staff appoint a DPO. One issue is how far the DPO may be personally liable for any breach in the law as opposed to the company itself. There is debate within the private sector whether a DPO should have a legal and regulatory background or an IT or a business systems background given the complexity of data transfer issues. And even within the EU different countries have different approaches towards monitoring and enforcement. For example, in Germany the DPO is more of a watchman than an advisor and is open to prosecution in cases of serious data breaches. In the UK the regulator does not proscribe the duties of the DPO, but does require them to register.[24]

Box 1: Australia - Sensitive Personal Data

I. Racial or ethnic origin
II. Political opinions
III. Membership of a political association
IV. Religious beliefs or affiliation
V. Philosophical beliefs
VI. Membership of a profession or a trade association
VII. Membership of a trade union
VIII. Sexual preferences or practices
IX. Criminal record

Some jurisdictions make a distinction between personal data and sensitive personal data. Personal data refers to information such as bank account and credit card numbers, medical records, personal identification and national insurance numbers, etc. These will usually be safeguarded in law, and any unauthorized attempt to circulate or sell this information would be a criminal offence. Cross-border data transfers will legitimately include such information in encrypted files for purposes of online bookings and e-commerce payments (credit card details), medical treatment abroad, etc., but only with consent of the individual.

[23] US International Trade Commission (2013) *Digital Trade in the US and Global Economies, Part 1* p.5-5 http://www.usitc.gov/publications/332/pub4415.pdf
[24] See *Computing* (13 Nov 2013) 'Rise of the Data Protection Officer' http://www.computing.co.uk/ctg/feature/2306122/rise-of-the-data-protection-officer

Sensitive personal data is a further category of data that some jurisdictions add that may be restricted from cross-border transfer, although it may consist of information which is nevertheless public knowledge. As with personal data, sensitive data requires individual consent before being communicated to third parties. The assumption of law makers is that sharing sensitive information may not be in the best interests of the individual.

As Table 2 shows below, half of the Asian economies listed do restrict sensitive personal data.

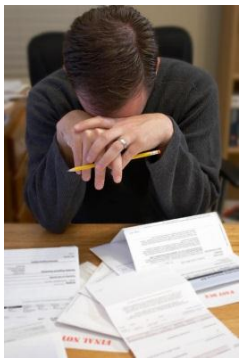
Table 2: Personal Data and Sensitive Personal Data

Country	Personal data defined (transfer with consent only)	Sensitive data defined (generally not for transfer)
Australia	Y	Y
New Zealand	Y	N
India	Y	Y
Indonesia	Y	N
Hong Kong	Y	N
Japan	Y	N/Y
Malaysia	Y	Y
Philippines	Y	Y
Singapore	Y	N
South Korea	Y	Y
Taiwan	Y	Y
Thailand	Y	N

Note: N/Y in the case of Japan means sensitive data is defined by the Japan Financial Services Agency's "Guidelines for Personal Information Protection in the Financial Field"

Running aside the issue of data *protection* is the issue of data *sovereignty*. The key issue here is who 'owns' the data. For example, does the patient or the doctor own a patient's records? In most jurisdictions the law interprets the patient as the owner and the doctor keeps the records on behalf of the patient and with the patient's consent. This will also apply to any sharing of the records. For example, when a doctor shares the data with another doctor it will be assumed that it is in the interests of the patient, but not necessarily so if the sharing is with a pharmaceutical company. And does it apply to the doctor's own personal notes about a case? In the case of data transfer out of the country to another jurisdiction the question of ownership will have implications for which set of laws and regulations apply. The normal assumption is that the laws in the jurisdiction in which the subject resides and/or in which the data was collected will apply, but that often has to be tested. If the subject lives abroad, if the data controller is from a third country, if the data was distributed by a third party without authorization, the situation can become legally complex.

A DPO?



Can a DPO really be on top of *all* of this, *all* the time for *every* country and *every* situation? The answer is clearly in the negative. Once again, the larger international Internet companies are more able to afford the services of specialist legal advisors across the region, and it is to their competitive advantage they do. For major business customers, as they engage in international commerce, having a greater degree of certainty about the legal protection of their data and their own liabilities if there should be any breach of data transfer regulations is part and parcel of the level of service they will pay for. If cloud service providers can offer that level of service they will have a competitive advantage over those who cannot.

E: APEC, EU, US AND OECD CO-OPERATION ON DATA TRANSFERS

APEC's approach to personal data privacy began to take shape in 2005 with the APEC Privacy Framework which "set out a set of nine principles to assist APEC economies in developing data privacy approaches that optimize privacy protection and cross-border data flows." In 2009, APEC ministers endorsed the Cross-border Privacy Enforcement Arrangement (CPEA) which creates a framework for regional cooperation in the enforcement of Privacy Laws. Any Privacy Enforcement Authority (PE Authority) in an APEC economy may participate.

Box 2: OECD Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data is the benchmark reference document. The seven governing principles for protection of personal data are:

1. Notice—data subjects should be given notice when their data is being collected;
2. Purpose—data should only be used for the purpose stated and not for any other purposes;
3. Consent—data should not be disclosed without the data subject's consent;
4. Security—collected data should be kept secure from any potential abuses;
5. Disclosure—data subjects should be informed as to who is collecting their data;
6. Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
7. Accountability—data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

Source: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part3

One of its aims is to "provide mechanisms to promote effective cross-border cooperation between authorities in the enforcement of Privacy Law".[25] This was followed in 2011 with a ministerial endorsement of a Cross-Border Privacy Rules (CBPR) system "designed to protect the privacy of consumer data moving between APEC economies by requiring companies to develop their own internal business rules on cross-border data privacy procedures." [26] This is similar to the EU system of Binding Corporate Rules (BCRs).[27] In May 2014, Japan joined the USA and Mexico in agreeing to implement the CBPR system under the guidance of the APEC Electronic Commerce Steering Group.

"E-commerce continues to develop rapidly to meet rising product and service demand among the Asia-Pacific region's 2.8 billion consumers," said APEC Electronic Commerce Steering Group Chair Lourdes Yaptinchay. "Complementary regulatory policy that limits costs to businesses while protecting data privacy is critical to facilitating this process."[28]

To date, Japan is the only Asian economy to have signed up to the CBPR which is slow progress after 3 years, but these have been the years of the Great Recession in the global economy, and with signs of a return to financial stability it is to the advantage of business and economies across the region to accelerate the process. Since 2013, following the revelations of Edward Snowden, there has also been an understandable wariness by all parties, with the danger that issues of national security get mixed up with the debates about how to facilitate cross-border trade-related data. The localization debate (see above) in particular has been clouded by these issues, which is why there is now some discussion

[25] See http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

[26] See http://www.apec.org/Press/Features/2013/0903_cbpr.aspx. The CBPR is a voluntary, certification-based system that promotes a consistent baseline set of data privacy practices for companies doing business in participating APEC economies. Company privacy policies are to be audited by APEC-recognized Accountability Agents. See http://www.apec.org/Press/News-Releases/2013/0306_data.aspx.

[27] Bilateral trade between the EU and ASEAN in 2011 reached over €200 billion (US$261 billion), one-third of it with Singapore which is also the region's data centre hub.

[28] https://www.apec.org/Press/News-Releases/2014/0501_CBPR.aspx

of partitioning off data related to national security issues in the same way special goods are isolated in a bonded warehouse system. This may be one way to refocus urgent attention on the need to free-up data transfers of a non-national security character.

At the multilateral level, since January 2013, APEC, the EU and the US FTC (Federal Trade Commission) have been working on ways to map BCRs and CBPRs onto each other. If successful, and if more law makers and regulators in Asia start promoting the use of CBPRs, this could lead to a less-stress approach to cross-border data transfers. Cooperation at this level has been very much part of the OECD agenda, with the OECD drawing particular attention to the still small number of cases in which international cooperation agreements between the EU and other jurisdictions have actually happened.

> "It is clear from the activities and reports of privacy and data protection authorities that they attach considerable importance to international and regional co-operation arrangements. It is also clear from the survey results that authorities do have concerns about their legal ability to take part in these joint activities. Where a legal framework exists permitting or requiring co-operation as in Europe, those arrangements are used in a small number of individual cases and to facilitate wider joint regulatory action. Given the overlapping membership among OECD, EU, Council of Europe, and APEC, continued information exchange and co-ordination of ongoing work will certainly be beneficial." (OECD, 2006)[29]

There are basically three broad categories of data privacy: personal, commercial and state.

- Personal data: a key consideration, especially on social networks, is whether the data on its own can identify an individual. In reality, given the power of search engines, almost any data can eventually be linked to an individual, so technology outstrips the intention of regulation.[30] In light of this, the OECD principles are not so easy to pin down in practice. A telephone number, for example, can be easily traced back to an individual and yet it would be impractical to ban the sharing of telephone numbers without the explicit consent of the individual. Ways to handle these problems tend to start with the "purpose" principle. If the purpose is telemarketing, for example, then the solution can be a Do-Not-Call register. It is important that working through these principles and finding solutions does not unduly interfere with the communications of information as opposed to its usage.

- Commercial data: protection is primarily the responsibility of the companies owning the data, but there are sector-specific areas in which national laws and regulations apply. These are sectors considered strategically critical to an economy or to social priorities, such as telecommunications, banking, health, defence, media, etc. A cloud service provider will win business, or lose it, according to the quality of service they can provide. This is especially true where the customers are international businesses, and data transfer laws and regulations

[29] OECD (2006) *Report on the Cross-Border Enforcement of Privacy Laws* pp21-22 http://www.oecd.org/internet/ieconomy/37558845.pdf

[30] For this reason the recent European Court ruling in favour of the 'Right to Be Forgotten', a provision already in place in South Korea, is considered by some to be outdated before it is enforced. It gives the right of individuals to have links on a search engine to items about themselves to be taken down if they are out of date or irrelevant and have no public interest element to them, all items that raise legal questions, such as when is something out of date or of no public interest? But the items themselves will not be taken down and search engines outside of Europe can still link, and they can still be accessed within Europe in a variety of ways, including over virtual private networks (VPNs).

that set the bar at a height that only multinational companies can jump over will disadvantage local and regional service providers. On the other hand, if law makers and regulators set out to favour local service providers over foreign service providers, for example, by imposing restrictive ownership rules on data centres and requiring localization, this will slow down the growth of international trade in goods, services and e-commerce. There is an inevitable trade-off involved. To avoid the worst outcomes, namely constraining foreign trade and investment, a balanced solution needs to be found.[31] The "bonded warehouse" approach to sensitive data is one way forward.

- State-owned data: divides into national security data and the rest, but some states define national security in very broad terms. For "the rest" such data is by definition subject to regulation as to who can transfer it, who can receive it, using which carrier and mode of transportation, etc., a frequent but not necessarily a commercial assumption being a requirement to use national rather than overseas service providers. National security data is not the subject of this paper, but the "bonded warehouse" approach would seem especially applicable.

It follows from the above that while (1) that there are a set of commonly accepted principles, for example, the need for individual consent, the need for private sector privacy policies, and in practical terms that sending data abroad has to rest to a high degree upon the good judgment of the data controllers themselves, subject as they are to litigation or to regulatory penalties; and (2) there is a common recognition that the facilitation of cross-border data transfers is an absolute requirement of global trade in goods, services and e-commerce; nevertheless (3) efforts to coordinate a consistent set of policies towards cross-border data flows are impeded, despite the benchmarks available from APEC and the OECD, by the variations that occur in in laws and regulations across jurisdictions; (4) cloud service companies are coming under more and more pressure to retain the services of a host of lawyers and compliance officers across many different jurisdictions just to keep up with the raft of new and revised regulations for different sectors of the economy, including codes of conduct and in some cases court rulings. This pushes up the cost of doing business as risk of violating data laws and a growing uncertainty over their interpretation increase.

Updating the Guidelines?

The OECD *Guidelines* refer back to a document that was drawn up in 1980 which has been the benchmark reference for the principles that guide national data privacy and protection laws. But there is now a growing argument for revisiting the *Guidelines* and the way in which its principles are made operational, because so much has changed in the IT world in thirty years. Most people have email addresses, increasing numbers have social networking accounts, many people shop online, and in all these cases they are leaving data trails. Big Data analytics has been evolved from its early days of search 'spiders' until today just about every usage of the internet and every connection to the Web means that an individual's data is being scooped up, stored and processed automatically. When Google vans take street-level images for Google Maps, passing individuals get recorded, and WiFi connections can be unintentionally captured. As countries make the shift to "smart cities" using sensors of all kinds, people's data can be caught, intentionally or otherwise. As the Internet-of-Things

[31] From the perspective of foreign companies and think tanks, the solution should be embodied in international free trade agreements. For one such advocate, see Joshua Meltzer (2013) *The Internet, Cross-Border Data Flows and International Trade* Brookings http://www.brookings.edu/research/papers/2013/02/25-internet-data-flows-international-trade-meltzer

(IoT) emerges, for example, short-distance radio tags in clothes, in consumer durables, in automobiles, mean that more and more personal data will be captured.

It becomes impractical and not feasible in such a world to obtain an individual's agreement at every point. There is just too much data of a personal nature being continuously monitored. For this reason, a growing number of data specialists are suggesting the *Guidelines* need updating to make them relevant and workable in a world of Big Data and the IoT. The suggestion is for a shift from a focus on individual consent, which becomes difficult to maintain, to a focus on how that data is to be used and who has the right to use it. This does not imply an abandonment of consent where that is a practical proposition. Recently a team at the Oxford Internet Institute (OII), supported by Microsoft, has developed these ideas into a paper, *Data Protection Principles for the 21st Century.* [32] The authors argue

> "To shift responsibility for data protection away from individuals, and to focus on data use rather than data collection, the revised principles make a significant distinction between principles that apply to data collection and those that apply to data use or other processing activities." (p.13)

They make the valid point that most users never read the small print of the privacy statements, they just click YES without really knowing what they have agreed to. By shifting focus onto usage and users (data controllers and processors which together they refer to as "data stewards") the burden of responsibility falls upon those who gain advantage from the use of data and who have the professional resources to monitor and safeguard data according to law.

The implication for data controllers at first sight seems to add to the burdens of compliance, but if it leads to a more comprehensive and transparent system of data control, it could be a blessing in disguise. The paper itself probably does not give enough support to the idea of harmonization of laws as it suggests that "achieving more – uniformity among the laws – is not only unachievable but also undesirable, given significant cultural differences." (p.14) Certainly, local laws will differ in details, but if as the authors suggest, a revised set of principles is warranted, it makes good sense to align the treatment of, for example, cross-border data transfers, as closely as possible. If not, the costs of compliance will rise.

Audit Trails

As concerns about breaches in data security and data protection mount, the importance of audit trails increases, and one of the concerns with cloud computing is how to ensure an audit trail exists. Although some jurisdictions give powers to the regulator to conduct an audit, notably in Australia, Indonesia, Malaysia and Thailand, in most economies there is no specific requirement.[33] But, as an OECD report noted, "[t]here is a growing trend to co-operate at the international level in regulatory investigations."[34] For example, in the EU the "Article 29 Working Group" sets criteria for auditing cross-border data transfers. It started by identifying private health insurance data for its first round of activity in 2005 and joint audits with Australia, Canada and the US on Passenger Name Records (PNR)

[32] http://www.microsoft.com/en-sg/download/details.aspx?id=41191
[33] ACCA (2014) *The Impact of Data Sovereignty on Cloud Computing in Asia,* country chapters.
[34] OECD (2006) *Report on the Cross-Border Enforcement of Privacy Laws*, p. 20 http://www.oecd.org/internet/ieconomy/37558845.pdf

data for airlines.[35] As referenced above, the collaboration between APEC, the US FTA and the EU "Article 29 Working Group" is another example.

However, the situation in Asia Pacific is not satisfactory if data controllers are left in limbo as to what is expected of them. One way audit trails are enforceable is through data retention requirements which, in the eyes of some, stand in contradiction to the concept of personal data privacy.[36] Whereas data privacy laws require data controllers to destroy the records once their stated purpose has been fulfilled, data retention laws often require telecom companies and ISPs to retain data for much longer periods. In the case of the EU Data Retention Directive of 2006, the requirement is from 6 months up to 2 years. Sector-specific regulation and local authorities can also require their own data retention periods. In the US, records of when and where calls and messages were sent is regularly collected on a global basis by the National Security Agency (NSA) because metadata is not considered 'data' under US law. Due to the fallout following the Edward Snowden revelations about the scale of NSA surveillance, President Obama announced that telecommunications data would in future be retained only by the carriers with data retention periods remaining as they have been under Federal law. One report suggested a "senior administration official said the phone companies would likely receive money to cover their compliance expenses, although the details haven't been worked out yet."[37]

In yet another recent development to complicate the picture for cloud service providers, the European Court of Justice in May 2014 decided to uphold the "Right to be Forgotten". In Asia, South Korea has a similar policy. Under the ruling, individuals will be able to request that search engine links to search results related to them, but which they consider out of date, irrelevant and of no public interest, should be removed. This does not remove the original search result, just the link to other results so the search process would become more lengthy and less revealing. Apart from the legal uncertainties posed by the decision – for example, when something may be considered "out of date" and of "no public interest" could be contested – the fact that it can only apply to search engines operating in Europe raises questions of cross-border by-pass of the law. This case raises the possibility that someone inside the EU using a virtual private network (VPN) could access a search engine outside the EU and download linked information about another person.

It is presumed, *but as yet untested*, that a cloud service provider acting as an intermediary would *not* be liable under EU laws. Intermediary liability is something that ISPs and other service providers have been strenuously arguing against, yet in several Asian economies, such as China and Vietnam and maybe now also in the Philippines, local ISPs are vulnerable. Any general shift toward intermediary liability would have very serious consequences, not just for the time-honoured *principle* of carrier and service provider neutrality, but for the cost and practicality of doing business. It would be far preferable if a common set of principles could be adopted to reduce the level of regulatory uncertainty in this area. The Asia Cloud Computing Association warns that:

[35] OECD (2006) *Report on the Cross-Border Enforcement of Privacy Laws*, p. 20 http://www.oecd.org/internet/ieconomy/37558845.pdf
[36] "National data retention laws are invasive, costly, and damage the right to privacy and free expression." https://www.eff.org/issues/mandatory-data-retention. The Electronic Frontier Foundation is an advocacy group.
[37] National Journal, *Obama Asks Congress to End NSA Mass Surveillance*, 27 March 2014 http://www.nationaljournal.com/tech/obama-asks-congress-to-end-nsa-mass-surveillance-20140327

> "The principles behind intermediary liability – that is, where intermediaries such as ISPs are held responsible for content transmitted over their networks – are now being looked at as the foundation for regulating user-generated content on virtual or cloud-hosted platforms."[38]

The chilling effect this will have upon ISPs and cloud-service providers will mainly affect *local* service providers who are dependent upon their home markets for commercial success.

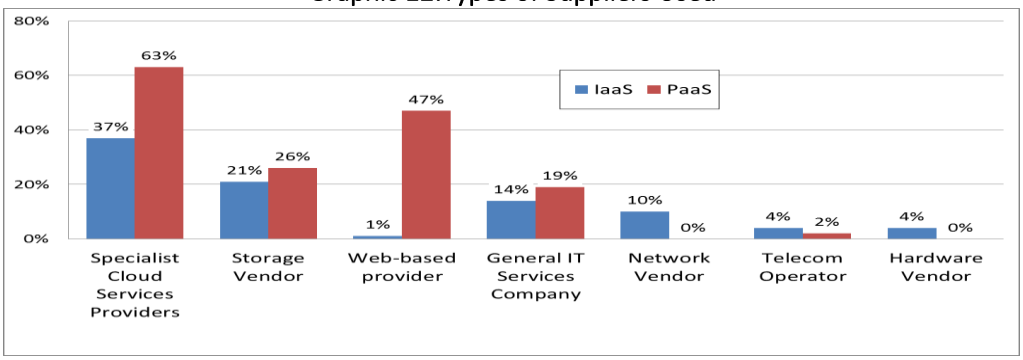
F: Telecommunications, Cloud Services and Data Transfers

The role of telecommunication carriers has, for obvious reasons, been central to the international movement of data, whether public or private data. Very few cloud service providers build and own their own networks, although the larger multinational Internet companies are beginning to do just that. Private networks are usually leased from telecom providers, often managed by them or provided by third party vendors, for example, as virtual private networks (VPNs) who use the networks of the telecom companies.

The Internet has changed the picture insofar as the data itself is no longer tied to a particular network. For public cloud services, digital bits fly off in all directions for reassembly at the terminal destination. Routing algorithms determine the least-cost and/or best quality global routes. But telecom companies, and their investments, remain at the very heart of the system of global networks that make all this possible. Nevertheless they have had to reinvent themselves in the face of the Internet, and an important part of that is to offer data warehousing, data management services and co-locational facilities and services based in the cloud.

In these markets, telecom companies are not the main players. Despite owning and operating most of the supporting network infrastructure, telecom companies have captured only around 4% of the IaaS market and just 2% of the PaaS market according one global survey of 700 companies, as illustrated in Graphic 12.[39]

Graphic 12:Types of Suppliers Used



Source: Joseph Waring, TelecomAsia.net, 9 April 2014, Telcos' place in the cloud, http://www.telecomasia.net/content/telcos-place-cloud

But telecom companies are considered data controllers. Apart from the data they collect from their own subscribers, such as usage and billing data, as cloud service providers they also handle their

[38] ACCA *Cloud Readiness Index 2012* p.15

[39] "Current Analysis surveyed 700 enterprises from around the world about their supplier preference for IaaS and PaaS now and over the next 12 months. The survey found that telecom operators have just 4% of the IaaS and 2% of the PaaS market." http://www.telecomasia.net/content/telcos-place-cloud

customers' data. In some cases they may go beyond mere carriage, they may process data, for example, by sorting according to type, destination, prioritization, etc. Therefore in economies that require a data controller to register, a telecom company does so.

The level of detail is high and how exactly that information will be used subsequently by the regulator is not yet clear. It is, for example, rather difficult to forecast for years ahead the exact nature of the data customers will want transferred abroad and to which destinations. Presumably, it will be the responsibility of the DPO to keep up-to-date with the regulator's requirements, for example, adding to this information over time and confirming whether certain categories of data are exempt or restricted and what circumstance must apply in each case. The Malaysia law also gives the regulator powers of entry and search without a court order, although it is presumed, but not yet tested, that such powers would be exercised only in the most exceptional, serious and urgent cases and that normally a court order would be required. What is clear is that where registrars exist, telecom companies, along with all other data controllers, will need to devote even more resources to compliance issues than already exist under the local telecommunications law.

Box 3: Malaysia: Registration Requirements

The following is a summary of the registration form all data controllers must complete to register under the Personal Data Protection Act 2010.

1. Details of company, type of business, etc.
2. Class of data users: (i) communications, (ii) insurance, (ii)health, (iv) transportation, (v) educations, (vi) banking and financial, (vii) direct marketing, (viii) services, (ix) real estate, (x) utilities, (xi) tourism and hospitalities
3. Purpose of collecting and description of type of personal data
4. List of persons/organizations to whom the data may be disclosed
5. List of countries to which the data may be transferred, directly or indirectly, including description of data and purpose of transfer
6. Name and contact details of the compliance officer under the Personal Data Protection Act 2010
7. Various documents, such as the Memorandum of Association

The telecom companies, if they are to compete effectively in the cloud services market, need to be on top of these issues. Even if their clients are primarily responsible for authorizing the data transfers, they too may not be fully aware of the legal and regulatory environment where the data is being transferred to. As clients they will often look to their cloud service providers for advice and guidance and see it as part of the quality and level of service they are getting. The more complex the rules over cross-border data transfer the more costly it becomes for service providers to comply and the advantage shifts towards those who can, who are almost by definition the giant multinational Internet companies and service providers. Local carriers and service providers will therefore be disadvantaged.

Codes of Practice

The complexity of compliance increases as the number of sector-specific areas where data privacy and protection regulations are introduced increases. One means of reducing the burden of compliance and therefore the cost of doing business is the industry code of conduct. An example of a regulator-initiated code of practice comes with the 2014 reform of Australia's Privacy Act 1988 where the new Part IIIA of the Act is accompanied by regulations and a new written code of practice about credit reporting, the registered credit reporting code (CR code).

Credit Reporting

When individuals move from one country of residence to another and then seek financial services such as a credit card, a property mortgage, the purchase of an annuity, the bank or financial institution will most likely revert to a credit reporting agency to check the credit history of the applicant. Keeping the databases up-to-date is essential for all the involved parties, and that is only possible if the credit reporting body (CRB) is able to transfer data across borders. In recognition of this, Malaysia for example, has exempted credit rating agencies under the Credit Agencies Reporting Act 2009 from cross-border data restrictions. Australia too. As part of the reforms to Australia's Privacy Act, credit reporting is now regulated by a new Part IIIA.

"Consumer credit"
A new term 'consumer credit' has been included in the new Part IIIA. The definition of 'consumer credit' expands on the definition of 'credit' in the old Part IIIA, which limits the application of the credit reporting provisions to credit that an individual intends to use wholly or primarily for personal, family or household purposes. The new term extends the application of the provisions to credit that is intended to be used to acquire, maintain, renovate or improve residential property for investment purposes, or to refinance such credit (s 6(1)).

The new Part IIIA permits five new types of credit-related personal information to be held in the credit reporting system:

- the type of consumer credit
- the day on which the consumer credit is entered into and day on which it is terminated or otherwise ceases to be in force
- the terms and conditions of the consumer credit that are prescribed by the regulations and that relate to the repayment of the amount of credit (ss 6N(b) and 6(1))
- the maximum amount of credit available under the consumer credit
- repayment history information (RHI), which is information about:
- whether or not an individual has met an obligation to make a monthly payment that is due and payable in relation to consumer credit
- the day on which that payment is due
- if an individual makes a payment after that day, the date on which that payment is made (s 6V).

Importantly, a credit provider can only disclose RHI to a CRB if they hold an Australian credit licence under the National Consumer Credit Protection Act 2009 (ss 21D(3)(c)(i)). Similarly, a CRB can only disclose credit reporting information that is, or was derived from, RHI to a credit provider that is a licensee under that Act (s 20E(4)). Although the RHI may relate to payments missed since 12 December 2012, credit providers will only be able to disclose that information to CRBs from 12 March 2014."

Source: http://www.oaic.gov.au/privacy/privacy-law-reform/credit-reporting-reform

Just how difficult it is to know exactly where the legal liabilities start and end is illustrated by two cases below. In the first case, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a company based in Belgium and which handles a high proportion of the world's financial transfers, was found subject to, and having violated, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

Case 1: SWIFT and Canadian Law
"[I]n *Privacy Commissioner of Canada v. SWIFT* (April 2, 2007), it was alleged that SWIFT, a company established primarily in Belgium and the United States, inappropriately disclosed to the US Treasury personal information originating from or transferred to Canadian financial institutions. The Canadian Privacy Commissioner determined that SWIFT was subject to the Personal Information Protection and Electronic Documents Act (PIPEDA) because the organisation operated in and was connected in a substantial way to Canada. She noted that SWIFT operates in Canada; collects personal information from and discloses it to Canadian banks as part of a commercial activity; and charges a fee to the banks for providing this service. Several of its shareholders and

one of its directors were Canadian. While acknowledging that SWIFT's operations in Canada make up only a small percentage of the organisation's global business operations, the Commissioner noted that SWIFT has a significant presence in that country and was therefore subject to Canadian law."
Source: http://www.hcch.net/upload/wop/genaff2010pd13e.pdf

The second case is of a lawyer from France caught between a rock and a hard place. Unwittingly, he broke French law on data transfer by complying with a court order in the USA.

Case 2: French Lawyer caught between French and US Law
A French lawyer was convicted in France of "the crime of disclosure of economic, commercial, industrial, financial or technical documents or information that are to constitute evidence for a foreign proceeding", when he sent documents to the U.S. pursuant to a U.S. court discovery order without receiving the proper consent in France to do so. This action, despite being required by a U.S. court, violated French law, and the French attorney was criminally prosecuted in France as a result. The resulting sanctions case went to the French Supreme Court, which upheld the conviction and the €10,000 fine. This may be the first case where a litigant has been tried in another jurisdiction for attempting to comply with a U.S. discovery order, but the example illustrates the importance of finding an appropriate balance between the requirements of effective cross-border judicial co-operation (in this case, the taking of evidence abroad) and data protection laws.
Source: http://www.hcch.net/upload/wop/genaff2010pd13e.pdf

Normally in law the liability will fall on the data controller who authorizes data collection and its subsequent usage, but it cannot be assumed that this absolves an agent of the data controller of breaking a law or regulation when transferring data to another jurisdiction, or as case 1 shows, brings immunity from laws in other jurisdictions. Nor, as seen in case 2, does it absolve a data controller or an agent who breaks the law by complying with court orders from another jurisdiction. In both the cases cited, at issue was the *interpretation* of laws and regulations as in neither case was there any evident intent to circumvent a law.

This can place cloud service providers, among others transferring data, in an invidious position, and a telecom carrier may well be both a data controller and an agent. As economies strengthen or introduce new laws governing sectors such as banking and health services, while the bank or the health service provider will be the primary data controller responsible for the protection of personal and sensitive data under both the sector-specific laws and the general law, a carrier offering cloud services to these organizations will also have to examine its need for compliance. In other words, not only are there many, and possibly conflicting, laws and regulations, but there remains a great deal of uncertainty and lack of clarity as to who is liable for what and to which regulator. This adds significantly to the costs of doing business.

A recent study by the Asia Cloud Computing Association created a scorecard of 14 Asian economies according to how clear and consistent were their laws relating to data sovereignty for cloud computing (Table 3). The scores for the cross border movement of data ranged from 87% for Japan down to 49% for China, and those for regulatory stability and enforcement from 88% in Australia, Hong Kong and Singapore to 59% in China.

Table 3: Index of clarity and consistency of laws relating to cloud computing

Economy	Cross-Border Movement	Regulatory Stability & Enforcement	Economy	Cross-Border Movement	Regulatory Stability & Enforcement
Japan	87%	76%	Taiwan	71%	66%
New Zealand	80%	82%	Thailand	71%	62%
Australia	76%	88%	Hong Kong	69%	88%
India	73%	66%	South Korea	67%	80%
Malaysia	73%	63%	Vietnam	66%	58%
Singapore	73%	88%	Indonesia	65%	67%
Philippines	71%	51%	China	49%	59%

Note: Extracted from 4.4 Scorecard results, ACCA (2013) *The Impact of Data Sovereignty on Cloud Computing in Asia*, p.12 – see http://www.asiacloudcomputing.org/research/datasovereignty2013

It is apparent that even in the highest scoring economies the situation falls short of perfect. Also, the freedom of data to transfer across borders with the least number of constraints does not apply specifically to the more developed economies, although Japan, New Zealand and Australia head the list. India, Malaysia, the Philippines, Taiwan and Thailand all rate above 70%. The real concern though is the column headed 'regulatory stability and enforcement'. Nine of the fourteen economies score below 80% and eight score below 70%. Regulatory uncertainty remains a problem.

G: Conclusions and Recommendations

> "Cloud providers and their customers are asking which governments have access to their data, and whose laws prevail, when it is hosted offshore. The lack of legal clarity is impeding the growth of the regional and global cloud markets." ACCA *Cloud Readiness Index 2014*

It is intuitively obvious, but also confirmed by numerous studies, that cross-border data transfers are a vital part of world trade. At the same time, the risks associated with breaches of personal data and sensitive data privacy are rising as it becomes easier to send and receive information over the cloud. For this reason, data protection laws and regulations are spreading to many sectors. The upside is that citizens and businesses should feel more secure; the downside is the cost of doing business is increased, in particular the cost of compliance.

A sensible objective is to achieve a balance between privacy, security and the free flow of information. A practical way to achieve this objective is a policy approach that distinguishes between different categories of data and applies different levels of security requirements to each. This will add an important level of certainty to the management of cross-border data transfers. And if all economies can align their regulations accordingly, including the adoption of a common terminology for data protection and categories of data, this will have two beneficial effects. First, it will greatly reduce the cost of compliance as well as helping cloud service providers avoid errors which often arise due to the complexity and obscurity of regulations. Second, it will assist regulators in cross-border collaboration, to resolve issues such as jurisdictional rights as well as promoting trade and solving cross-border crime.

Sometimes called a granulated approach, it is one that uses the principle of proportionality, one that does not impose unnecessary costs on enterprise. If the approach starts with the purpose for which

the data is to be used and who will be accessing it, then categories that suggest themselves are from the highest levels of regulation to self-regulation:

- issues of national security, such as communications between embassies, military communications, etc.;
- sensitive data that either cannot be taken out of the country or has to fulfil special conditions, such as an 'opt-in' arrangement;
- personal private data where consent is understood to have been given or other conditions apply, such as the fulfilment of contract conditions, and confidence that the data is being sent into a jurisdiction where data protection is equivalent;
- non-personal data which is subject to contractual agreements with downstream data controllers and third party users which conform to the requirements of regulators, such as APEC's CBPR, especially if these can be extended to include third parties;
- data that is proprietary to the data controller, and does not fall within any sector-specific regulation.

This paper recognizes that developing economies in particular have good reasons for wanting to protect the data of their citizens and have an interest in assisting the development of their own domestic cloud service providers and data centre operators. Some economies, such as China, Indonesia and Vietnam, have already started down this path. This paper disagrees with the view expressed in one part of an otherwise helpful report by the U.S. Chamber of Commerce, that "it is more effective to demonstrate the flawed reasoning behind the laws and persuade policymakers to repeal them altogether, than attempt to find common ground on the localization issue."[40] On the contrary, policymakers in these economies have their own reasons to pursue a local development strategy and should be aware that there are costs involved in localization policies.

What those costs will be is inevitably speculative and based upon assumptions. Equally, they should review how easily it will be to realise benefits in terms of promoting local cloud service providers, and policymakers should be open to more flexible policies.[41] In particular, the cap on foreign direct investment (ownership) of local data centres is something that should be reviewed on the understanding that foreign majority ownership is usually the pre-requisite for more overseas investment, the introduction of more innovation, more intellectual property, and a greater transfer of technology and skill sets. On the contrary, where FDI is constrained to less than 50 per cent, the sustainability of the joint venture is far more difficult to achieve.

Recommendations

1. All economies in the region sign up to the APEC Cross Border Privacy Rules, appoint Accountability Agents, and support efforts to align such arrangements across regions.
2. All economies that introduce the CBPR, and who recognize the use of company contracts as a vouch-safe for the protection of the data when it is taken out of the country, should permit them

[40] Hunton & Williams (2014) *Business without Borders*, p. 18 U.S. Chamber of Commerce. This publication provides a good analysis of why many of the arguments for localization are flawed – see https://www.uschamber.com/sites/default/files/documents/files/021384_BusinessWOBorders_final.pdf

[41] For China and Indonesia especially, the size of the local market is an important consideration.

to be sufficiently flexible to include sub-contractors and third parties and transfers to multiple parties.

> "As one company representative said 'Data transfer agreements contain impractical clauses that don't work well in a large multinational – e.g., a customer right to approve subcontractors.'… Standard contractual clauses generally work best for linear transfers of data from point A to point B. Their rigid structure is not well suited to the web of data transfers and onward transfers between service providers and subcontractors, which frequently occur in a fluid basis, particularly in cloud-based platforms." [42]

3. Once a contract has been approved, similar contracts should receive automatic approval unless important changes are introduced for a specific data transfer.
4. Economies should make serious efforts to introduce a harmonization of terminology and definitions in their laws, regulations and into standard contracts. This will go a long way to reducing levels of obscurity, confusion and therefore uncertainty. A standard contract with standard terminology and wording should be made available to data controllers in each economy. Economies should encourage industry sectors to establish their own voluntary code of conduct in discussion with regulators.
5. Economies should introduce a series of data categories that correspond to different levels of data protection and cross-border regulation. Although exceptions are always possible, the costs of compliance will be lowered if some uniformity of approach can also be introduced to sector-specific regulation, using as far as possible the same categories.
6. As there are several aspects to achieving regulatory goals where business and technology intersect, economies should look to leveraging technical solutions where possible, such as protecting data transfers using common encryption standards. While this may not address all regulatory concerns, it effectively ensures the control of, and access to, data remaining within jurisdictional boundaries, and is an example of a verifiable technical solution to a regulatory objective.
7. Data privacy and protection issues are also the subject of bilateral, regional and multilateral trade agreements. Unlike many elements of such agreements which are contentious and subject to "horse trading", cross-border data transfer should be regarded as a win-win issue as part of a trade facilitation process. Data centre localization should be regarded as a tangential yet separate issue and disagreements over that should not retard agreement over trade facilitation issues.
8. An approach to localization that would minimize its negative consequences for cross-border data flow is to treat data centres as if they were "bonded warehouses". Within the data centre, high-security data categories would be quarantined for inspection, some to be embargoed, others to be processed until cleared for transfer, the rest to be passed through the Green Lane.
9. Economies with FDI caps on data centre ownership should give serious consideration to lifting the restrictions, and if necessary imposing contractual obligations to safeguard local and national interests.

[42] Hunton & Williams (2014) *Business without Borders*, p.31: U.S. Chamber of Commerce. See https://www.uschamber.com/sites/default/files/documents/files/021384_BusinessWOBorders_final.pdf

ACKNOWLEDGEMENTS

The Asia Pacific Carriers' Coalition and the Asia Cloud Computing Association would like to acknowledge members of both organisations who assisted in the preparation of this report in their individual capacities. This report was originally commissioned by the APCC to TRPC Pte Ltd, and builds on original research developed by the ACCA as part of a broader and ongoing study on Data Sovereignty throughout the Asia Pacific, which is available at at http://asiacloudcomputing.org/research/datasovereignty2013

About Asia Pacific Carriers' Coalition (APCC): The APCC was formed in 2004 to promote and assist in the development of open market policies and telecommunications regulatory frameworks in the Asia Pacific region. APCC provides a point of industry contact with Governments and National Regulatory Authorities (NRAs), including through participation in public inquiries and consultations. We are committed to participating meaningfully in national policy discussions, regulatory processes and other forms of industry discourse. Our membership is drawn from the major global and regional telecommunications carriers operating in the Asia Pacific; and our association provides a forum for members to identify and examine regional matters of common interest affecting the industry and regulatory practice. Contact us at secretary@asiapacificcarriers.org or http://www.asiapacificcarriers.org

About the Asia Cloud Computing Association (ACCA): The ACCA was established in 2010 as an industry association comprising the stakeholders of the cloud computing ecosystem in Asia. The ACCA works to ensure that the interests of the cloud computing community are effectively represented in the public policy debate. Our primary mission is to accelerate the growth of the cloud market in Asia, where we promote the growth and development of cloud computing in Asia Pacific through dialogue, training, and public education. Through regular meetings, we also provide a platform for members to discuss implementation and growth strategies, share ideas, and establish policies and best practices relating to the cloud computing ecosystem. Contact us at info@asiacloudcomputing.org or http://www.asiacloudcomputing.org. You can also join us on LinkedIn at http://is.gd/accacloud

---

About the authors: TRPC is a specialist technology research consultancy with over 25 years' experience in the Asia-Pacific. We offer specialized advisory, research and training services with a focus on regulatory and strategic business issues, possessing an extensive regional network of industry experts and professionals. Our research focuses on the economics and business strategy of telecommunications and information technologies, as well as the policy and regulatory issues associated with national information infrastructure development. http://www.trpc.biz