BRIEFING NOTE

ISOC-TRPC-IIC Roundtable on Privacy in an Internet of Things World

Prepared by TRPC Pte Ltd.
Introduction

Today, we live in a world where connected devices outnumber humanity, and as we usher in the age of the Internet of Things (IoT) where every device - and increasingly every thing – is connected, we find that the gadgets around us are constantly collecting, transmitting, and analysing data. Up-to-date, contextual information tailored for the individual leads to better-informed decisions and choices, which could lead to greater empowerment.

At the same time, we find the very concept of privacy is being challenged because of increasing ease in which vast volumes of data can now be collected, analysed, and used. In the past the issue was comparatively simple: what privacy policies dictated what was offered and what we give up to access the offers. This meant a relatively clear delineation of roles and common definition among regulators, businesses and consumers on what privacy is and how data can be used.

That era is fast disappearing. While IoT and Big Data analysis allow businesses the opportunity to personalise their interactions with consumers by offering more context-aware products and services, the same opportunity can set businesses in direct opposition to consumers’ desire for privacy.

Furthermore, the growing sophistication of data analytics means that the capability already exists to identify, connect and mine personal information out of the aggregated data. Concurrently, the means to break data encryptions and security coding became commoditized and more widely available. We have entered a new era in which existing privacy policies are insufficiently flexible and robust to be effective.

Privacy and Data Protection

Personal privacy and data protection are two separate but inextricably linked issues. Data protection is about the unauthorised access of data, and notably about cybercrime involving the stealing of data which has now reached an industrial scale worldwide. Personal data privacy is about the unauthorised use of a person’s data by an organization that has been given that data in confidence and without permission to share it without the individual’s knowledge and consent. What links these two issues is that as cybercrime becomes ubiquitous, organizations are increasingly less able to guarantee the privacy commitments and undertakings they give in good faith.

There is a spectrum of personal data privacy violations that occur. At one end of the scale is the duplicity of some data controllers to ‘monetize’ the data they have collected from customers and users by selling it. If the data is truly aggregated in such a way that it is ‘anonymous’ then that is regarded as commercially acceptable, but there is a thin line between ‘anonymous’ data and data that can be easily cross-tabulated against other sources of data, for example on social networks, and individuals readily identified, including their contact details and their personal histories, for example their medical condition, their sexual orientation, their political views, etc. At the other end of the scale is organized crime where personal data is stolen, either from data controllers, such as banks, retailers and credit card companies, or from individuals. At the time of writing, in the UK it is
revealed that webcams used inside residences, for example, to keep an eye on a sleeping child, that are connected to the Internet are being hacked and the video images, complete with identification of the locations, are being posted on websites.\(^1\) And recently it was reported that even offline computers that have been compromised by software can be hacked by modified smartphones that can pick up FM transmissions from computer monitors.\(^2\) While the initial hacking innovations may be used by national security forces, they quickly become available to ‘black hats’ and well as to ‘white hats’.

As the means of cyber intrusion are becoming ever more sophisticated and widespread, so too are the opportunities for cyber intrusion as every aspect of modern living is somehow or other connected to the Internet and therefore interconnected across the Internet. In many cases, professionals can just as easily by-pass firewalls as they can the front door lock of a house. Two obvious developments that are opening up the opportunities are **Big Data** and the **Internet-of-Things** (IoT). Big Data, however it is defined, is really about analytical techniques to discern patterns that are not immediately obvious in a mass of data, often from a variety of different sources. The advantages are considerable, both for commercial enterprises and for public services, such as building smart cities, combatting diseases, and the like. Separately, the IoT is a development that is being led by the consumer goods markets, such as wearable devices, connected TVs, etc., although hidden from public view there is an even larger machine-to-machine (M2M) infrastructure market ready be a fundamental part of the IoT. The IoT will be an important feed into Big Data.

These developments leave nothing immune from cybercrime. That doesn’t mean that everything using Internet is likely to be compromised, but everything using Internet is potentially open to compromise. This undermines the approach to personal data protection that has become worldwide best practice up to date, namely based upon individual consent. The focus has to shift to the data controllers and their responsibilities and liabilities for the data they collect and store and use. Since they can no longer guarantee absolute safety and confidentiality, they must be judged upon their efforts to minimize risk, their response to breaches of security, and their degree of transparency in dealing with such breaches. Industry codes of conduct as well as laws and regulations should reflect this new reality. Countries who are considering introducing laws for personal data protection should take advantage of having an advanced perspective on these issues.

For the corporate enterprise and state sector, the issues are even more serious because of the public harm that can be caused by cybercrime. Of course, the financial damage is one aspect, but if infrastructure is compromised or public trust is undermined, the consequences will be far more damaging. There is no alternative other than a tiered approach to identifying the levels of risk consequent upon cybercrimes occurring. At the lowest level, insurance can be matched with evidence of the security levels adopted. Credit card companies adopt this approach, for example. At a higher level, the very architecture of the security apparatus may require overhaul and become a mandatory requirement. This could apply to banks, for example. At the highest level, a duplicate backup network unconnected to the operational networks that use the IP-enables networks, including secure and closed-user group networks, could be the way forward. But even off-line computers can be compromised without the tightest of security – see above. It is an expensive

---

\(^1\) See [http://www.bbc.co.uk/news/technology-30121159](http://www.bbc.co.uk/news/technology-30121159)

option, but compared with the cataclysmic risk of utilities going down it may be the prudent way forward.

This is not meant to overstate the challenges and risks. These are cost-benefit calculations, except that the unexpected nevertheless needs to be factored in. On a day-to-day operational basis, the enormous benefits that developments such as cloud computing are bringing to enterprise and the economy-as-a-whole need to be supported in tandem with a general cyber-security awareness. But at the same time, policy makers need to consider how best to manage cyber-security information, whether, for example, to impose transparency upon corporate entities by requiring them to report cyber-attacks, at least to an authorized body, and how to coordinate across borders, in ASEAN especially with Interpol’s new regional HQ in Singapore, and to harmonize national approaches to information sharing and law enforcement. And for the public, how to provide reassurance that personal data privacy remains an absolute commitment, but one that requires a shift in emphasis from the personal data-data controller relationship to the data controller-data user relationship.

There will never be easy answers to these questions, and while the questions may remain the same, the answers will change over time. The key will always to be to keep abreast of what they may be.

The OECD Template

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.

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. In light of this, the OECD principles are not so easy to pin down in practice. A

---

http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldatatemplatepart3

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
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 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. 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 (i) 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 (ii) 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 (iii) 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; (iv) 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.

---

5 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](http://www.brookings.edu/research/papers/2013/02/25-internet-data-flows-international-trade-meltzer)
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 a revisiting the Guidelines and the way in which its principles are made operational, because so much had 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 (IoT) emerges, for example, short-distance radio tags in clothes, in consumer durables, in automobiles, so 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, an growing number of data specialists are suggesting the Guidelines need updating to make them more 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. The 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. 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 makes 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.

**Personal data, sensitive data and cross-border data**

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.

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 1 shows, half of the Asian economies listed do restrict sensitive personal data.

**Table 1: Personal Data and Sensitive Personal Data**

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

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”

**Australian Definition of Sensitive Personal Data**

- Racial or ethnic origin
- Political opinions
- Membership of a political association
- Religious beliefs or affiliation
- Philosophical beliefs
- Membership of a profession or a trade association
- Membership of a trade union
- Sexual preferences or practices
- Criminal record
**Data Sovereignty**

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.

**Data Protection Officer (DPO)**

The European Union is proposing all companies employing more than 250 staff appoint a DPO. One issue is how far the DPO may be personal 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.7

Can a DPO really be on top of all the compliance issues, all the time for every country and every situation? The answer is clearly in the negative. 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.

**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.

---

One of its aims is to “provide mechanisms to promote effective cross-border cooperation between authorities in the enforcement of Privacy Law”.\(^8\) 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.”\(^9\) This is similar to the EU system of Binding Corporate Rules (BCRs).\(^10\) 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.”\(^11\)

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 in particular has been clouded by these issues, which is why there is now some discussion 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


\(^10\) 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. [https://www.apec.org/Press/News-Releases/2014/0501_CBPR.aspx](https://www.apec.org/Press/News-Releases/2014/0501_CBPR.aspx)

---

Briefing Note - ISOC-TRPC-IIC Forum on Privacy in an IoT World, Dec 15, 2014 @ Bangkok, Thailand | 8
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)

**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. But, as an OECD report noted, “[t]here is a growing trend to co-operate at the international level in regulatory investigations.” 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) data for airlines. 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. 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 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.”

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

---


16 “National data retention laws are invasive, costly, and damage the right to privacy and free expression.” [https://www.eff.org/issues/mandatory-data-retention](https://www.eff.org/issues/mandatory-data-retention). The Electronic Frontier Foundation is an advocacy group.

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:

“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.”

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.

---

18 ACCA Cloud Readiness Index 2012 p.15
Conclusions

1. Personal data protection laws have generally followed the OECD template which places the onus upon the data controller to seek the explicit permission of the data subject for the collection and use of their data. In a world of Big Data and the IoT this may no longer be a sufficient protection because data controllers will become less able to deliver on their commitments.

2. An alternative approach more focused upon the ways in which the data controller uses the data, including issues such as efforts taken to protect the data, the transparency of the processes used, efforts to explain data privacy policies in plain language that users can readily understand, an assessment of the risks involved, etc., may be required.

3. The appointment of data protection officers is a requirement in some jurisdictions, but smaller companies especially will have difficulties meeting the costs of compliance, as will companies operating across numerous jurisdictions.

4. Industry codes of conduct, negotiated with the sectors involved, could be a way forward, where compliance to the code of conduct will reflect upon the levels of liability of the companies involved in data losses and breaches of privacy laws.

5. Harmonization of policies towards personal data protection across jurisdictions can reduce both the costs of compliance and the likelihood of breaches of local laws.

6. Countries which have yet to adopt personal data privacy laws have the opportunity to frame them in ways which are most relevant to contemporary risks of data losses due to malpractices and cybercrime. This implies modifications to the OECD template.
TRPC offers consulting on economic and industrial research for the Asia Pacific Region. We focus on the economics of telecommunications and information technology, as well as policy and regulatory issues associated with national infrastructure development, with an emphasis on the South East and East Asia region.

Visit us at http://www.trpc.biz or email us at info@trpc.biz