East meets West: striving to interoperable frameworks?

The EU Article 29 Working Party and the Asia-Pacific Economic Cooperation launched their Referential assessing the similarities and differences between their two cross-border data transfers mechanisms on 6 March 2014. The Referential between Binding Corporate Rules (BCRs) and the Cross-Border Privacy Rules System (CBPRs) marks an important first step for the two regions to consider global interoperability. Malcolm Crompton, Managing Director at Information Integrity Solutions, examines the two frameworks individually and explores what the Referential could mean for the future.

Shortcomings of transfer solutions

The EU's Data Protection Directive (Directive 95/46/EC) places restrictions on the transfer of personal data about Europeans to places outside of the EU. With the growth of these transfers, the EU has developed solutions aimed at allowing appropriate transfers to take place more easily but still safely from the end user perspective. However, many of the potential solutions have substantial shortcomings:

- Meeting the EU's adequacy requirements – This is intended to be the default method, although in practice very few jurisdictions have been found to have laws that the EU deems to provide 'adequate' protection of personal data compared with the Data Protection Directive.
- US-EU Safe Harbor agreement – This allows organisations to self-certify as meeting the adequacy requirement. The arrangement is limited to companies in the US and has faced criticism from the EU regarding compliance and enforcement, to which the US is currently preparing a response.
- Contractual clauses – This could be seen as a fallback position that could be burdensome for companies engaging in extensive data transfers and hence requiring extensive contractual negotiations. From a business perspective the 'standard contractual clauses' developed by the EU authorities have not significantly alleviated this burden.

EU BCRs

Introduced in 2003, BCRs are a newer alternative aimed at allowing a multinational company to overcome problems of jurisdiction and friction. BCRs are internal rules adopted by a company which define its global policy with respect to the transfer and handling of personal data within the entire corporate group. Once approved by the relevant EU Data Protection Authorities (DPAs), an entity can send personal data anywhere in the world, as long as the receiving party is a member of the same corporate group and each party is compliant with the Data Protection Directive.

According to the EU Commission, in the 11 years since their introduction, 53 companies have adopted BCRs, including major firms across a range of industries such as American Express, Citigroup, Intel, Linklaters and Shell.

APEC CBPR

In the last 10 years, APEC has made steady progress in establishing a regional privacy framework, culminating in the CBPR System. The system allows private sector organisations in participating Economies to transfer personal data to each other, and comprises of the following:

- Internal rules voluntarily adopted by organisations (and on behalf of their subsidiaries/affiliates) for a uniform approach to the management of personal data;
- Privacy protection in line with the APEC Privacy Framework in addition to any local requirements (that is, local laws requiring a higher standard must still be complied with);
- Establishment of Accountability Agent(s) in each participating Economy to certify the organisations' rules, monitor and enforce compliance, and resolve disputes between individuals and organisations; and
- Privacy Enforcement Authorities (PEAs) in each participating Economy that must belong to the Cross Border Privacy Enforcement Arrangement (CPEA). This enables cooperation in relation to privacy investigations and enforcement matters, in particular where 'first line' enforcement by Accountability Agents has not resolved the difficulties.

Since its announcement in November 2011, take-up of CBPR has been slow, as it has been with BCRs. The United States became the first participant Economy in September 2012, with Mexico joining in January 2013 and Japan following suit in May of this year. Canada has submitted its application, while Australia and New Zealand among others are showing interest.

IBM became the first company to be certified under the CBPR System in August 2013, followed by Merck, a multinational healthcare company, in November. In March this year, two more companies

gained certification, perhaps indicating growing momentum.

The CBPR System differs from BCRs in its scope of operation. A company adopting BCRs is adopting a self-contained arrangement within its corporate group, but without geographic limitations. On the other hand, when fully implemented the CBPR System is designed to work across organisations, but is limited to participating organisations in participating Economies.

Currently the biggest challenge for the CBPR System is reaching the critical mass necessary for the system to prove its worth. This stems from a chicken-and-egg problem: Economies are slow to move without industry pressure for them to participate, while private sector organisations do not see a pressing need to join when the system is comprised of few Economies.

Going forward, sustained efforts are required on the part of CBPR policymakers to highlight the benefits, as well as to offer incentives, for participation. As with any network effect, once more players come on board, the value and appeal of the system will increase accordingly.

Towards interoperability?

In light of the data-driven global economy, the gold standard is a truly global framework for the safe and efficient transfer of personal data across borders. While realistically this remains a distant prospect, we consider that the two regional approaches of BCR and CBPR are logical starting points. Encouragingly, over the past year we have seen increased dialogue between the EU's Article 29 Working Party and APEC's Data Privacy Subgroup.

We consider that the release of a Referential on requirements for BCRs and CBPRs ('the Referential') jointly produced by the two parties represents a constructive first engagement in the work that must commence eventually on global interoperability. The document itself is quick to point out that it is not aimed at mutual recognition. It describes itself as an 'informal pragmatic checklist' that identifies separate and overlapping requirements for organisations seeking certification under one or both systems.

A cursory glance at the Referential comparing the BCRs and CBPRs gives the impression that the two systems are quite different, with some lengthy treatments of clarifications and additional elements. However, we would suggest a more careful reading, bearing in mind that the length is often due to the direct reproduction (and repetition) of paragraphs from supporting reference material. Furthermore, a useful comparison must take into consideration the intent and purposes behind the respective requirements, as well as their potential practical effects.

Any framework for the safe and efficient cross-border transfer of personal data must have the following features:

- A baseline level of privacy protection that follows the data
- Expressed through internal rules and policies
- Enforced via accessible redress mechanisms when something goes wrong
- Demonstrated through initial and ongoing methods.

Looking critically at the BCR and CBPR systems, we consider that there are fundamental similarities and surmountable differences that make greater interoperability eminently achievable in the future.

A baseline level of privacy protection that follows the data

Meaningful privacy protection requires at least minimum standards to be met (or exceeded). Both the EU's Data Protection Directive and the APEC Privacy Framework have common principles based on the influential OECD Privacy Principles. These include, for example, fair and lawful collection, purpose specification, notice, data quality and data security.

The Data Protection Directive also contains principles not addressed by the APEC Privacy Framework, for example restrictions on processing of sensitive information and the right to object to automatic processing. The EU's General Data Protection Regulation, if and when it comes into force, may introduce new ones such as the 'right to be forgotten.' Any interoperability effort will need to bridge this gap.

An important aspect to cross-border privacy protection is that it must travel with the data so that individuals are not left without remedy because their data is in another location. Both the BCR and CBPR systems allow the transfer of personal data to other jurisdictions only if the recipient protects the data in way that does not diminish the original level of protection.

Expressed through internal rules and policies

Privacy protection needs to be operationalised via an organisation's internal rules and policies. Both the BCR and CBPR systems require:

- Training and oversight of employees;
- Designating individual(s) to be responsible for overseeing privacy compliance within the

organisation; and
- Setting up a clear complaint handling process.

Enforced via accessible redress mechanisms

Under the heading 'Remedies for Data Subjects and Third Party Beneficiary Rights', the Referential did not find any common elements between the BCR and CBPR systems. Procedurally speaking this is true but it arguably obscures the key point – whether enforceable redress is available and accessible.

The BCRs require that the organisation grant individuals the right to enforce its privacy rules as third-party beneficiaries, via one of the following routes:
- The jurisdiction of the data exporter located in the EU;
- The jurisdiction of the EU headquarters or member with delegated responsibilities; or
- Before the competent national DPAs.

These mechanisms ensure that European data subjects are able to obtain redress from a European entity, even if the breach occurs outside the EU.

The external enforcement process in the CBPR System starts with the Accountability Agent, who is responsible for investigating and resolving disputes between individual complainants and the target organisation. Where the problem is unable to be resolved and there is a violation of privacy law, the matter may be escalated to the PEA, who may coordinate with PEAs in other jurisdictions through the Cross Border Privacy Enforcement Arrangement in order to investigate and enforce the privacy breach.

It is important to note that despite the procedural differences, the underlying principle is the same for both the BCR and CBPR systems: the sending company should be accountable for the information that it transfers outside of the EU or APEC Economy, and the individual should be able to gain accessible redress for violation of any relevant privacy protections. BCRs achieve this by specifying one responsible EU entity. The CBPR System does so by fostering cooperation between Accountability Agents and PEAs in the APEC Economies where the transfer takes place.

The future of any interoperability effort for the safe and efficient transfer of personal data across borders is far from certain. However, the BCR and CBPR systems are surely part of the bigger journey that the world is taking towards that goal.

Demonstrated through initial and ongoing methods

Increasingly there is recognition that organisations must be accountable for their privacy policies and practices. This is being demonstrated worldwide by the actions of privacy regulators but is also being expressed in law. The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada has explicit accountability requirements, as do the new Australian Privacy Principles in Australia's recently amended Privacy Act 1988. The current drafts of the new EU Data Protection Regulation also introduces the concept of accountability very explicitly. Simply put, they are responsible for doing the right things as well to stand ready to demonstrate that those things are being done. The onus is on the organisation to comply with the law and build trust with its customers.

Both the BCR and CBPR systems are designed to ensure organisations are accountable for their privacy program. The first step is the initial certification process, where all the relevant requirements must be addressed and then assessed by the relevant body (DPA or Accountability Agent). Once the organisation is certified, both systems provide for ongoing monitoring and audit.

The BCRs require that an audit program be implemented – either on a regular basis or on specific request by the privacy officer – that covers all aspects of compliance with the BCRs. DPAs may also conduct audits and issue binding advice. In the CBPR System, participating organisations are required to attest on an annual basis to its continuing adherence to the program requirements. The Accountability Agent is then mandated to conduct regular comprehensive reviews.

Conclusion

The future of any interoperability effort for the safe and efficient transfer of personal data across borders is far from certain. However, the BCR and CBPR systems are surely part of the bigger journey that the world is taking towards that goal.

Conceptually speaking the CBPR System is an unequivocal improvement for participating organisations seeking to transfer personal data across APEC Economies with low friction, as well as for individuals who retain and can enforce the protections that follow their data. Reaching a critical mass of participating Economies and organisations has to be the top priority for CBPR proponents.

Will the CBPR System work? Will it facilitate cross-border commerce and make people's lives better? The proof of the pudding will be in the eating, and there are sure to be valuable lessons to be learnt along the way as APEC's cross-border framework proceeds inevitably forwards.

Malcolm Crompton Managing Director
Information Integrity Solutions
mcrompton@iispartners.com