RCEP: Handling Data Privacy

The Importance of Data Flows

Data is essential to economic growth in the digital age. Research by the McKinsey Global Institute has shown that access to open data can produce $3 trillion in additional value annually to the world economy, and that data flows now exert a larger impact on GDP growth than trade in goods. Businesses that trade across borders—both large and small—rely on data flows to communicate with customers and take advantage of low-cost technology options, especially cloud computing.

Maximizing data flows should be a policy priority for any country that seeks economic growth in the digital age.

But recognition of this objective does not automatically mean that privacy concerns are suddenly irrelevant.

Data Protection Best Practices

Many countries already have comprehensive privacy laws and regulations in place. Finding an appropriate or “best practice” policy on data protection turns out to be more challenging than it first appears.

Part of the difficulty is that different jurisdictions have already begun to implement diverse regulatory frameworks for managing data protection.

As an example, the United States has no overarching data protection provisions, but rather allows federal, plus state level, regulations. The American approach and style is different from the European Union. In both places, however, the overriding purpose—to respect consumer choice—is the same. Harmonizing these different approaches to meet the same common purpose is difficult.

In Asia, the most comprehensive set of policies can be found in the APEC Privacy Framework. The Framework sets out a series of principles to guide APEC members in collecting information. It provides both a set of legal principles and a commentary to help member economies decide how these principles might be effectively implemented.

The APEC framework does not take a one-size-fits-all approach or prescriptive approach. Rather, the framework allows a diversity of privacy laws while maintaining a consistent data protection and enforcement mechanism based on the principles. This respects members respective privacy frameworks, while at the same time allowing for data to flow and economic growth to be protected.

Key elements of the APEC Framework are the proper role of the privacy information controller, the importance of preventing harm through misuse of information, the procedures the needed to collect information and the proper notice required when collecting information, and the recognition that the right to collect information is limited only for necessary purposes, that individuals should be given a choice to participate, that information should be kept with integrity and security, and that individuals should be able to access and correct the information. APEC members approved the Framework in 2005.

---

1 Open data: Unlocking innovation and performance with liquid information, McKinsey Global Institute, 2013
3 http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx
The Cross-Border Privacy Rules (CBPR) system expanded on the Framework.⁴ The CBPR System consists of four elements: (1) self-assessment; (2) compliance review; (3) recognition/acceptance; and (4) dispute resolution and enforcement.

**The Important Role of Companies**

Whatever policies are put in place, clearly good data protection policies need to ensure that once data is collected, that firms that collect information have procedures in place to address requests for access to personal data, have data security measures in place, are held accountable for data security and data storage, have procedures for disposal, and manage corrections to data.

Adding to the complexity of crafting sensible data policies, some of the recommendations that appear to be common sense are actually likely to be less practical over time.⁵

For example, one basic idea is that consumers should provide written consent whenever data is collected—further, this consent should clearly inform consumers about the purpose for which the data is being collected, used or disclosed. Obtaining written consent in advance may make sense in some applications.

But as internet enabled devices proliferate, it becomes more and more difficult to obtain consent in advance. As an example of the practical problems that might be encountered, how will consumers provide written consent for data to be collected from their toaster? Does the toaster have to have a keypad built in? Does it need to have a smartphone app that needs activation before the first piece of bread can be toasted? In short, in an increasingly wired world, obtaining written consent for every possible use of data will be harder to obtain.

Flexibility is important. For example, a “legitimate interests” clause could allow data processing without consent when there is a good reason to do so under certain circumstances.

If formal consent is not needed for every transaction, then it is necessary to have some sorting mechanism to decide what types of data need consent and what types of data do not. This is a difficult determination for regulations to meet in advance. Recall again that some devices can be reconfigured in the future as well, making it possible that some items might cross the threshold for needing consent at some point.

In order to craft sensible regulations, governments will need close cooperation with industry as the sector is evolving rapidly. The types of data collected, the kinds of privacy issues that arise, and the need for consent are likely to change. RCEP will need to include feedback mechanisms to ensure that provisions for data protection and privacy remain relevant.

**The Need for Coordination**

As data becomes more and more prevalent in different aspects of our lives, it is important that privacy measures have a strategic basis and do not proliferate in an ad hoc manner. One practical policy recommendation is to have one central agency or department at the domestic level have responsibility for data privacy issues - or at least a high level of coordination among respective government agencies - to avoid creating additional confusion and policy fragmentation in data protection and privacy rules.

---
