Privacy, Cybersecurity, and the Internet of Things in Asia: What to Expect in 2019

14 January 2019

Increasing numbers of initiatives, devices, and solutions related to the Internet of Things (IoT) are substantially impacting the development of cybersecurity and data privacy regulations throughout Asia. After the implementation of the General Data Protection Regulation (GDPR) in Europe, for example, Asian lawmakers are considering strengthening their own data protection laws. The region is also characterized by a push in a number of jurisdictions towards data localization requirements driven more by "cyber sovereignty," national security considerations, and protectionist impulses than data protection considerations. Restrictions on the collection and free use of data may pose a challenge for IoT models, particularly if data is required to be kept onshore.

At the same time, it is clear that many Asian jurisdictions see IoT as a key driver for economic growth. A number of jurisdictions have "smart city" initiatives and interests in areas such as automotive telematics. Japan, South Korea, and China, in particular, have strong automotive sectors and are focused on maintaining technological leadership. Unmanned aerial vehicles (UAV) are also an area of focus, both in terms of the supply of vehicles and components and in terms of their deployment as part of these "smart" initiatives.

In this hoganlovells.com interview, Mark Parsons, a Hogan Lovells partner based in Hong Kong, summarizes the current status of IoT-related policies in the Asia-Pacific region and discusses changes anticipated in 2019.

Will Europe's stringent data protection regulations have an impact in Asia?

Mark Parsons: Definitely. We have observed a trend toward comprehensive, European-style data protection regulation here in the Asia-Pacific region for over a decade now and the introduction of the GDPR has given lawmakers fresh cause to consider if they have gone far enough in this direction.

China introduced an information security specification in May of 2018, which borrows quite heavily from the GDPR in terms of substance. It's a nonbinding national standard, but we're finding that enforcement authorities are referring to it when enforcing more generally worded

provisions found in mandatory Chinese laws. And India — also a significant economy in the region —has tabled a draft privacy act that also borrows heavily from a number of the innovations in the GDPR.

This is important to IoT considerations, and the rise of mandatory data breach notification laws in the region is a significant development. As an example, we now have six jurisdictions with mandatory regimes. We have volunteer regimes in three of them, and quite likely a number of these volunteer regimes will harden into mandatory regimes in the coming years.

A key consideration for these breach notification laws is the threshold for notification — do data subjects have to suffer harm in order for the breach to be notifiable, or is *any* leakage of personal data notifiable? Part of the European influence we are seeing is in the movement from a harm-based threshold to the standard under the GDPR. We see that influence in South Korea, the Philippines, and a number of other jurisdictions that have put in place mandatory regimes. So again, there are very significant developments on that front.

Have data localization requirements in Asia impacted data protection and cybersecurity laws?

Parsons: We are very focused on the emergence of data localization requirements. There are businesses with IoT offerings that just will not work unless they locate servers in jurisdiction (and obtain necessary licenses to do so). This can be a significant cost and a very important operational constraint for IoT models in the region.

We see China as the most significant marker on this front, where for a year and a half now we've had a localization measure under the cybersecurity law that has not yet been fully specified. We are still awaiting the fine print on who this measure applies to and what the procedures are in terms of complying with it. We're seeing similar movements toward localization in other markets, such as Indonesia. The new draft Indian law also contains a form of localization measure.

How does China's regulatory landscape compare to others in the region?

Parsons: China's data regulation landscape is a complex overlay of regulations that look at different types of data and industries. I mentioned two types of data — medical and location — that regularly come up in the context of interesting IoT deployments for China. Those are examples of areas where there are specific regulations dealing with the collection and handling of that data in addition to the restrictions found under the data protection and cybersecurity laws.

The regulatory complexity in China goes far beyond data, particularly now with the geopolitical tensions at play. China is obviously a very attractive market, given its scale and how wired its economy has become. For IoT-based businesses there are telecommunications regulations and other areas of regulation to contend with. Given the foreign investment restrictions in force in

China, businesses may have to partner with a domestic Chinese company, forming a joint venture, or deploying some other structural solution to bring their technology and services into the country.

What about Asia's regulations regarding drones and automotive use cases?

Parsons: Drones and automotive are two very exciting and interesting areas in this part of the world.

We've seen a fairly steady movement toward civil drone regulations. Jurisdictions such as China, Hong Kong, and India have regulations in place that generally have been led by civil aviation authorities with a primary focus on safety and national security rather than on privacy and data protection concerns. We're not yet seeing, for example, cybersecurity or data standards evolving specifically in these jurisdictions in relation to drones.

And we can't ignore the trade issue. Certainly the fact that a number of Chinese manufacturers are leading in this area is raising supply chain and national security issues in the West in the same way that network equipment has. So that's an important point to watch for.

How important is the IoT to the region's automotive industry?

Parsons: This part of the world — Japan and South Korea, in particular, as well as China — has a number of substantial automotive industry leaders. These jurisdictions are seizing on that strength and looking at the next generation with telematics, self-drives, and other applications. Part of their IoT ambitions is clearly focused on automotive, so there is a big push.

We have other jurisdictions, such as Singapore, that are not leading carmaker jurisdictions but have great technological ambitions. Singapore sees autonomous drive as part of its "smart city" initiative. Singapore has authorized a number of trials and is encouraging R&D and investments in IoT-connected vehicle applications.

You've said that the rise of industry standards in Asia will be interesting to watch. Why?

Parsons: Because right now, the status quo certainly is very much a patchwork of standards — where standards exist at all, to be frank — and I'll be interested to hear from the other regions as well. We see that various national laws are effectively influencing standards development. China's cybersecurity law is a good example, where technical specifications for information security being developed for network infrastructure are having impacts on IoT.

But apart from that, the field is still open. There has been fairly concerted activity by other jurisdictions that have tried to pave the way for interoperability and set common baselines in areas such as cybersecurity. Japan's General Framework for Secure IoT Systems is a good example, and that's been in play now for a couple of years, although it is a very general and high-level framework.

We note the GSMA has been working with a number of regional operators on developing IoT standards that will support interoperability between and amongst networks. We see government-supported activity in this area in Singapore, Japan, and South Korea in particular — again, jurisdictions that either have an interest in supporting the growth of the technology industry or are exporters of equipment and technologies that are likely to prosper in a more open IoT environment.

About Mark Parsons:

Mark Parsons is a TMT partner based in Hong Kong, with a practice spanning the Asia-Pacific region. Mark's practice covers the full range of commercial and regulatory work in the technology, media, and telecommunications sectors and other business sectors that depend on technology, media, and telecommunications to reach their customers and manage their operations. His practice reflects increasing convergence within the TMT sector and the increasingly important interfaces between TMT and financial services, retail, automotive, and other sectors.

Contacts

Mark
Parsons

Partner

> Read the full article online