IoT Cybersecurity and Data Privacy Trends in Asia: Be Ready

13 June 2017

In this hoganlovells.com interview, Hong Kong-based Hogan Lovells partner Mark Parsons talks about the regulatory environment in Asia as it relates to cybersecurity, data privacy, and the Internet of Things (IoT).

Can you tell us about developments in the Internet of Things (IoT) with regards to the Asian market?

Parsons: There is great enthusiasm for the IoT across Asia. There are many jurisdictions in the region that are seeking to be IoT leaders. In advanced consumer markets such as Hong Kong, where I live, the focus is on developing a smart, connected city, and so there is a lot of official encouragement, investment, and development of the IoT. Also, the regulatory environment is different from the U.S. and Europe. It is less advanced in terms of understanding the risk and the management of risk within the IoT.

The other major dynamic is that Asia — China in particular — is also the world's primary manufacturing base for many of the connected consumer goods that are — or will ultimately become — part of the IoT. The regulations directed at ensuring that these products are safe and secure is behind the risk curve right now. But it's catching up fast. There is no other choice.

Are there any recent changes to law that will impact connectivity and the IoT in Asia?

Parsons: The primary step forward is through data protection legislation, where increasingly we have what I would call "European-style" regulation in most of the major regional economies. Secondary concepts are being picked up, with the lead again coming from Europe where the General Data Protection Regulation (GDPR) has been confirmed and will be implemented in 2018. That has resulted in raised awareness among consumers across the Asia-Pacific region.

While data protection law is now a familiar feature on the Asia-Pacific regulatory landscape, cybersecurity law has lagged behind. The game changer for the region is China's Cyber Security Law, which took effect on June 1st 2017. It has been very challenging for even close observers to understand the precise impact of China's Cyber Security Law, but it is relatively clear at this stage that many businesses operating IoT infrastructure in mainland China will be considered "network operators" that will be subject to additional regulation. It is possible that IoT infrastructure

operated by key industry players, such as energy and transport, could also be considered to be part of something called "critical information infrastructure" under the new law, which attracts an even more stringent level of regulation. We are still waiting on detailed implementing regulations to understand the full impact.

Is regulation moving fast across Asia?

Parsons: I think with regards to broader legal issues like product liability and litigation, we have not seen a movement towards mass litigation yet. But lawmakers are moving towards providing wider scope for class actions, more rigorous rules around product recalls, and stricter labeling legislation.

In terms of cybersecurity, we've seen the greatest advance in financial services, which has been more of a focal point in terms of hacking and is otherwise a very sensitive sector in terms of the importance of financial systems and the sensitivity of the data processed in those systems. At the same time, consumers in the region are very enthusiastic about digital banking, mobile payments, and e-commerce, and this has led to a stepping up of regulation in this area in many markets. But we don't think it will stop at financial services. Those standards are important in their own right but they will also have an impact across the board, and the cyber-readiness will bring everything else up to speed.

Is there anything specific you track to indicate progress?

Parsons: We see data breach notifications as an interesting bellwether to watch for as legislative environments evolve. If there is an obligation to notify consumers or regulators, that really drives the compliance picture forward. It means a more active enforcement environment where risk and rights are being better protected. It also means greater publicity around data breach incidents.

With the Dyn attack last year, we had a particularly high-profile data breach concerning IoT. The impact was largely felt in the United States, but many of the compromised IoT devices that enabled the attack were reportedly manufactured in China. The incident highlights that IoT risk issues are global in their dimensions, and lawmakers everywhere should be moving to avoid being the weak link.

About Mark Parsons

Mark Parsons is a TMT partner with a practice spanning the Asia-Pacific region. His practice covers the full range of commercial and regulatory work in the technology, media, and telecommunications (TMT) sector and in other business sectors that depend on TMT 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