Data protection and breach notification legislation strengthens across the Asia-Pacific region

13 September 2017

In this hoganlovells.com Q&A, Hogan Lovells partner Mark Parsons discusses data privacy and cybersecurity trends and the evolution of laws and regulations in the Asia-Pacific region.

What is the status of cybersecurity and data protection regulations in most Asia-Pacific countries?

Parsons: The shifting landscape in cybersecurity and data protection regulations across the region is a very hot topic.

Asia as a region has lagged behind Europe, in particular, in terms of the development of updated data protection laws. The last few years have seen a real rapid pace of development in this area. We've actually had a number of jurisdictions — Australia, New Zealand, Hong Kong, and Japan — which have had data protection laws for quite some time. These are advanced, European-style comprehensive data protection laws, based on the 1980 Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

The Asia-Pacific Economic Cooperation (APEC) Privacy Framework was released a few decades after the OECD model. What was its purpose, and what impact has it had?

Parsons: There was a bit of a time lag there; the APEC Privacy Framework came through in 2005. Under this, the APEC member economies agreed upon a framework for developing a uniform standard of data protection law across the region. And the focus here was economic; the focus is on building consumer confidence in e-commerce and across border-data transfers, and achieving that through agreeing a common standard of data protection compliance across the region.

What we saw in the aftermath of the APEC Framework was a flurry of new comprehensive laws across the region. South Korea, Taiwan, the Philippines, Malaysia, and Singapore have now all adopted comprehensive European-style data protection laws.

What is the European style of data protection?

Parsons: The European model is a consent-based model for data protection regulation where data is regulated on the basis of general data protection principles across industry sectors without distinction.

So with that, we'll also mention India. India is not an APEC member, but it, too, joined the comprehensive regulatory fold in 2011 with the introduction of its Information Technology (IT) Rules, which also introduced formal data protection regulation to India.

Closer to home, how does China's approach to data protection compare to other countries?

Parsons: China's approach to data protection regulation is more sector-based, but we have seen a move towards more comprehensive regulation in China, with potentially overlapping laws across sectors and fields of activity. Financial services, telecommunications, and the Internet led the charge with sector-based data protection regulations around 2011 and 2012. We saw the introduction of a nonbinding but comprehensive national standard in 2012, which has been influential on how businesses are approaching data protection in China. Then, with the passage of amendments to the Consumer Protection Law in 2014, we see a much broader-based approach to data protection in the consumer space.

China does not yet have comprehensive data protection legislation, but how effective is its cybersecurity law?

Parsons: Most recently, we've had an intense focus on the Cyber Security Law (CSL), which came into effect on June 1, 2017. We are still waiting to see detailed implementing regulations from many of the provisions under this law, but certainly the level of activity we've seen in response to this law is impressive.

It's clear to us that businesses across a range of sectors are focusing far more closely now on data protection issues in China, and on related technology procurement issues and data location issues. So the upshot there is that we now have a dedicated regulator in China — the Cyberspace Administration of China — which has as its sole focus cybersecurity issues. And that sharpening of focus is important.

Are mandatory breach notification requirements becoming increasingly commonplace across the Asia-Pacific region?

Parsons: An important barometer, I think, for talking about what businesses are doing in service of addressing the compliance requirements for data in cyber is looking at data breach notification requirements.

Countries like South Korea, Indonesia, the Philippines, and Australia do have mandatory data breach notification requirements.

In China, Hong Kong, Singapore, and Japan there are sector-based mandatory notification regimes. Hong Kong and Singapore also have voluntary breach notification regime across all sectors.

The trend here, again, is definitely toward more and more breach notification.

What does this mean, in real terms?

Parsons: It means that you have regulators becoming aware of more breaches sooner, and you have individuals becoming more conscious of breaches and cybersecurity issues, whether directly through having had their data compromised or learning about breaches through the media. The trend is towards mandatory breach notification laws. The European General Data Protection Regulation (GDPR) will, next year, introduce a 72-hour mandatory breach notification requirement. We've already seen that requirement replicated in the Philippines in the implementing rules and regulations that were introduced there at the end of last summer. So the trend is to take inspiration from these advanced European requirements and replicate them in the region.

We would point out that, even in the absence of a mandatory breach obligation, there may still be a need to notify impacted individuals so as to reduce the impact of a legal obligation to handle data securely. For example, if credit card details have been compromised, there may well be a legal requirement to notify the consumer that that's happened so that they can take steps to cancel the card, even if there isn't a mandatory breach requirement.

More broadly, we do see clients wrestling with these issues, because there is a matter of reputation and good practice and brand messaging around privacy, where it may well be important to notify the consumer no matter what has happened. And in terms of notifying regulators, I think there's an important calculus to be made about whether the regulator is going to learn of the breach through complaints or through the press. Having a proactive approach to engaging with the regulator may be a good idea even if there is, strictly speaking, no obligation to notify them.

What is your definition of the "new normal" in data protection?

Parsons: When I say, "Welcome to the 'new normal,'" I mean that hacking incidents are obviously increasingly frequent, increasingly sophisticated, and may expose increasingly sensitive and valuable data.

Engaging with consumers digitally, which most of our clients in most sectors are now doing, presents great opportunities, in terms of reaching consumers at the right time and in the right place. But remote access through mobility creates new potential "weak links." It exposes consumers to new interfaces with your business that can be spoofed through phishing scams and so on. And business models leveraging cloud and mobile solutions can also raise new weak links in terms of third-party systems and interfaces that the client does not directly control.

So the punch line here is that data protection and cybersecurity are definitely increasingly board-level issues for organizations across a wide range of business sectors. We do see focus on and recommend that time be spent looking at these issues.

About Mark Parsons

Mark Parsons is a technology, media, and telecom (TMT) partner based in our Hong Kong office 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 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