Jennifer Stoddart
May 16 2014

Driving excellence through Data Governance

1. The changing data protection and privacy landscape

When I first became a privacy commissioner, in the province of Quebec in Canada, it was the summer of 2000. At that office there was only one computer that was wired into the Internet, considered a dangerous place. And of course no one had heard of the word Google. As for tweeting, only the birds did that .

How things have changed! Today almost all government and private sector business is conducted on line, linked to public and private information clouds. And changing communication modes so drastically calls for new rules .So Singapore has to be congratulated for joining the group of

80 or more countries world wide that have adopted data protection rules.

While the next panel will discuss in more detail the implications of data protection for the future, i would like to set the new Singapore law within the recent past and within global developments.

I will address briefly four aspects of data protection which are shaping our informational world, both for business and for personal internet users. They are: consumer data protection trends, transborder data flows,the European Directive on Data Protection, and harmonised enforcement.

Consumer data protection trends

As you know, consumers now use their devices to browse goods and services, order products for delivery, do their banking, play games and connect with friends and family. Here in Asia, doing all this from a mobile device is extremely popular.

In order to maintain consumer trust in what is, after all, unseen and incomprehensible to most, clear rules are necessary. This is where data protection comes in. For an

economy to fully reap the benefits of Internet business, it must create a framework in which business has clear rules for all to follow and in which consumers feel confident that their data is secure. This is the background to the huge increase in data protection laws, particularly in jurisdictions where trade and commerce are important economic drivers. Which brings me to my next topic, trans border data flows.

Trans border data flows

Information jumps, at a click , from one side of the world to another. In another jurisdiction, half a world away, what assurance does the consumer have about how this information will be treated? Who may be reading my health records, analysing my credit card purchases or parsing my e mails? Will it be a government or a corporation or both? Or , god forbid, a hacker who has just broken through some weak corporate firewalls.

These concerns have led some countries to put conditions on data export. There are a range of approaches to these international flows of data, all of which seek to ensure the safety and integrity of the exported personal information.

Singapore s new law has adopted the more flexible accountability approach like the Canadian laws, relying on a chain of obligations attached to the data as it travels abroad for processing or use. This puts individual businesses on the spot for making sure, when data changes hands, the next organization observes identical standards.The two different approaches to allowing data flow leads to a discussion of the European Directive and the forthcoming European Regulation.

The EU : from directive to regulation

The European union has set the gold standard in data protection. Its rules are the most demanding for organisations to comply with, calling for an investment in privacy specialists, lawyers and technologists to craft practices adapted to the line of business of each company. Soon the EU hopes to adopt a new Regulation on data protection, aiming to simplify compliance for companies doing business in several EU countries and yet posing hefty fines of up to millions of euros for non compliance.

Data export from the EU is subject to approval from the local country regulator unless the country to which it is destined

has a similar regulatory framework and privacy standards to that of the EU.

The desire to simplify the regulatory burden for international trade prompted Canada to adopt a private sector data protection law as early as the year 2000. When the EU recognised this law as being up to its own standards, as it has done more recently for your neighbour New Zealand, it was called " adequate ". Note this term. I m sure you will hear a lot about it in the future.

Cooperative Enforcement

As the use of the Internet increased dramatically in the new millennium, personal information was increasingly scattered around the globe, often in branches or subsidiaries of the same global enterprise. Different regulators in different locales were each responsible for some part of the enterprise. Not hard to imagine what happened when something went wrong, like a massive data breach. Which regulator should act? All or some ?

Regulators have different powers. For example, some could compel evidence, some could not. Some could impose fines, some had only their moral authority to publicly denounce problems.

The need for coordination was obvious. And so today regulators in Europe , Asia and the Americas communicate almost constantly on common data protection challenges, like the introduction of a new product, such as Google Glass or the repetition of inadequate privacy policies by some international entities.

A recent example of co operative enforcement is the joint investigation by the Dutch and the Canadian authorities of the popular application What 's App whose customer base numbers in the millions and which is currently being acquired by Facebook.

Even within Canada different authorities co operate on identical goals. One of the first of these joint Canadian investigations was led by Commissioner Denham when she was at the province of Alberta data protection authority. She worked with my office on the well known case of the data breach of the company T. J. Maxx in 2007. The victims of

the data breach turned to the Alberta commission for help. It in turn teamed up with the federal office which was responsible for international action.

Her investigation proved decisively that this global corporation had consciously made the decision not to bring its encryption strength up to industry wide revised protection standards. You can imagine the lawsuits and the compensatory payouts that flowed from that.

About 4 years later, the ringleaders of the criminal group which had hacked into the company were apprehended and are now in jail in the United States.

2 Challenges of embracing personal data protection in a digital world

The challenges for businesses now subject to data privacy laws are considerable but they are not insurmountable. Businesses which aim to be viable outside their own countries will soon realise that data protection is now an integral part of global commerce. Companies based in Singapore are fortunate to have a law which is flexible and administered by an agency which has done its homework very thoroughly.

I would recommend that before the law comes into force, you do a privacy impact assessment to see how your operations may use (or misuse, as the case may be)personal information. Commissioner Denham will speak more about this later. Make the necessary changes in your information handling practices or computer programs.

But above all, train your staff. Make sure every employee understands that protecting personal information is an integral part of his or her job. Name a chief privacy officer and ensure that this person has the authority to do the job well.

Conclusion

Singapore s new law is built on a solid foundation of data protection principles. I believe it is adaptable to business needs for a manageable regulatory burden. Its presence will allow companies to be active in new markets which demand the safe and confidential use of personal information.

Overall, this law will contribute to Singapore s prosperity and I congratulate the ministry of Communications and the Data Protection Commission for taking this important initiative.

Thank you.