UNSW – Cybersecurity, Privacy and Big Data

Speaker: Sven Bluemmel, Information Commissioner

Date: Tuesday 17 July, 2018

Opening remarks – cybersecurity, privacy and big data

Good morning everyone and thank you to the University of NSW for having me here to open the seminar program for today.

I am delighted to be here to speak with you as Victoria's inaugural Information Commissioner – and what an exciting time it is to be in the information policy and oversight space. Since the inception of the Office of the Victorian Information Commissioner, or OVIC, in September last year, we have seen an enormous amount of change in the information law landscape already, both locally and internationally.

In my role, I am supported by two Deputy Commissioners. Rachel Dixon is the Privacy and Data Protection Deputy Commissioner. Acting in the role of Public Access Deputy Commissioner is Joanne Kummrow, who is responsible for Freedom of Information. Together, Jo, Rachel and I are supported by about 50 staff.

Our Office, OVIC, has combined oversight of FOI, privacy, and data protection, administering both the Privacy and Data Protection Act and the Freedom of Information Act here in Victoria.

This morning I would like to share some thoughts on today's theme: cybersecurity, privacy and big data.

First, I think it's crucial that we acknowledge the landscape we're navigating at the moment. With the European Union General Data Protection Regulation now in full swing, many companies and organisations are grappling with legal areas that have previously not been an issue. Aside from the legal side of things, we are witnessing exponential growth in various forms of technology that are producing and using more diverse and complex data, blurring the notion of what is and is not personal information.

For example, improvements in artificial intelligence technology are providing increasingly sophisticated way to analyse and unlock the value of big data that were previously unrealised. This brings with it immense opportunity and also uncharted territory for both privacy and security considerations in a legal and practical sense.

We need to keep in mind during today's discussions that we don't yet fully know how all of this is going to play out. The technology landscape is developing faster than ever before, and this is occurring against a changing legal backdrop. It's important that government, business and industry are equipped to manage this context as changes occur.

Cybersecurity

Now, it's important that we consider what we're talking about when we talk about cybersecurity. This term is not consistently defined in the industry, and while work is being undertaken by standards committees to resolve this, it is incredibly important to define the term in the context in which is it being used.

For instance, if 'cybersecurity' only refers to attacks from the internet, then threats and vulnerabilities from other vectors may be missed when identifying design, organisational and operational risks, as well as the resulting risk management plans.

As a general rule when talking about protective data security, we cannot and should not limit our thinking to ICT security. By limiting our focus to cyber threats, we overlook the remaining security domains (physical, information, personnel) as well as governance. By doing this, we make ourselves vulnerable to unconsidered risks (e.g. a malicious insider, human error, physical attacks or unauthorised access).

In the context of big data, cybersecurity is of course a key element in a strong risk management plan, but we would be doing ourselves, and the individuals providing their data, a significant disservice by limiting ourselves to that.

So while we focus the discussion around cyber today, we should always remember that good, robust security is about much, much more than that.

Privacy

Second, when considering privacy, it's really about a lot more than a compliance exercise or preventing breaches. It's also about creating and maintaining a relationship of trust with those whose information you are using.

A big part of this is about being transparent – we have all seen recently in the fallout over Cambridge Analytica and Facebook, that when individual expectations about their information don't align with company practices, this can be extremely damaging. This also highlights that just because you can do something with data, it doesn't necessarily mean you should.

There is no point developing systems that are unsecure or that people don't trust – so making privacy and security core features rather than add-ons when using data will assist organisations to develop (and maintain) this trust.

The Information Privacy Principles are strongly aligned with good information management practices – embedding them in from the beginning will not only help you comply with the Privacy and Data Protection Act, it will also make your life easier down the road from a business information management point of view.

Any time you're thinking of using personal information within a big data context, it's important to ask the question – what is the problem we're trying to solve? And who is that problem being solved for?

If you can solve that problem without using so much information, you should only use the information that is necessary. If the problem you're trying to solve is your problem, and not one of the individuals' whose data you're using, it's worth considering if you do in fact have a the 'social license' to undertake the project.

Big data

I turn now to big data and the promises that come with it these are of course very alluring, and it's easy to fall into the habit of trying to solve problems by throwing more data at them.

But we also have to remember that it can be easy for data to be manipulated or 'massaged' to produce the desired results. Big data analytics and their models are rarely, truly neutral and never 100% accurate – so we need to keep in mind that just because big data is being used, it doesn't automatically eliminate the risk of bias, mitigate the status quo, nor prevent those with a particular agenda from achieving their objectives.

Remember that technology is only as good as the information you feed it – if you are using old, outdated

datasets, or datasets containing inherent biases, you will create systems that replicate or exacerbate these issues. Always question your data, where it is coming from, and how it may be having unintended consequences.

What has this got to do with privacy and security?

Information privacy is valuable for reasons beyond just compliance with privacy law – it also provides the basis of a good ethical framework when working towards a 'data driven culture'. Moving beyond the confines of thinking of privacy as strictly about collection, use and disclosure of personal information, the benefit of working with the privacy principles is that it can help mitigate the potential negative consequences in instances where the use of data analytics has led to the development of a system that ends up being used in different ways to what they were designed for.

Robust security protocols and risk management practices go beyond preventing security incidents – they are also just really good business practices, saving money and time in the long run.

Any conversation about big data needs to take into account the technologies that come with it. That means data linking and matching, predictive analytics, machine learning and deep learning, neural networks in all of their variations, biometrics, as well as de-identification and re-identification. Each of these areas have their own privacy and security considerations that organisations need to think about when employing emerging technology.

Conclusion

As I conclude my remarks, it's encouraging to see so many people gathered to discuss privacy and security together – as those topics are often divided. Approaching big data from a holistic information management approach will mean that more risks are identified and mitigated ahead of time, with protections built in rather than tacked on at the end.

While the focus is primarily on the legal side of things here today, we need to remember that we also must consider the technical and social considerations when using big data. Data does not exist in a vacuum, and the way it is used can have real and lasting impacts on individuals, beyond the economic consequences for companies. So, if you remember nothing else from me this morning, I encourage you to remember the human side of data.

I trust you will have an informative and productive seminar. Thank you.