Interview with David Watts, Commissioner for Privacy and Data Protection Victoria

Sharon Givoni *SHARON GIVONI CONSULTING*

Sharon: ***Tell us a little bit about your role.***

David: My role covers the traditional privacy responsibilities — assurance, dispute resolution, oversight of the public sector's privacy practices, as well as more recent data security functions. These cover developing, overseeing and monitoring a set of Victorian Protective Data Security Standards for the Victorian Public sector.

Sharon: ***Has the new role provided challenges, what was your experience negotiating them?***

David: There have been many but they involve two key themes. The first has been to re-conceptualise public sector privacy. It had gained an undeserved reputation for stifling innovation. The second has been coming to grips with emerging technologies which undermine traditional notions of privacy.

One of the key issues for the Victorian public sector has been information sharing, particularly to respond to the risk of family violence. In order to undertake proper risk assessments in the family violence area, personal information needs to be shared. There are a number of barriers to sharing personal information, but privacy law is almost never the cause.

People do not share information for a variety of reasons, including legislative confidentiality and secrecy provisions, policy and cultural reasons. Transforming a culture that resists appropriate information sharing is difficult; it needs ongoing commitment. To support this process, we have issued guidelines about information sharing. We have also developed a downloadable, interactive information sharing tool that guides the decision-making process.

Cultural change does not come easily and the regulator cannot achieve it alone. It requires concerted effort from all stakeholders. Disappointingly, sustained senior executive support has been slow.

From a security point of view, Victoria's track record has been poor. In the past, Victoria has directly adopted Commonwealth security standards without proper consideration of the needs of the state. These needs differ to those of the Commonwealth. It has a broader range of responsibilities like national security and foreign affairs. States are primarily concerned with delivering services like policing, child protection and education. Our approach has been to tailor the Commonwealth's Protective Security Policy Framework to meet Victorian needs while remaining consistent with the Commonwealth's approach.

The other main problem in Victoria is that the approach to security has been compliance-based. This has meant that the focus is on specific security measures (such as firewalls or passwords) and the use of checklists and certifications. Compliance-based approaches are now considered out-of-date. The Victorian Protective Data Security Framework is risk-based and focuses on a process-oriented approach. Each agency needs to undertake a risk assessment, then develop a security plan and implement security measures proportionate to its specific functions and activities and the security threats that it faces.

Sharon: ***Do you feel that there is a main thrust of those standards in terms of what they do?***

David: Security is often misconceptualised, focusing exclusively on confidentiality. There are three key dimensions to security:

- confidentiality;
- integrity; and
- availability.

We all understand the confidentiality dimension of security. But information integrity is equally as important. It emphasises the need to have reliable and accurate information. This concept is mirrored by the data quality principle in privacy law. Many government databases have never been cleansed and contain erroneous or incomplete information. Finally, availability ensures the right people have access to the right information at the right time. These three dimensions are what protective data security is about.

The Victorian Protective Data Security Standards mandate a risk-based approach to protective data security by establishing minimum security standards across each of the key security domains. These are:

- Governance
- KT Security
- Information
- Personnel
- Physical

Sharon: ***Is there anything similar to the New South Wales government in the pipe line for Victoria around the methodology of open data? What are the initiatives around collecting and anonymising data?***

David: The Victorian Government has announced it will be establishing a data centre for big data analytics capacity. The key issues about an initiative like that centres on governance, transparency and accountability.

The use of advanced data analytics also raises privacy and security issues. These include information self-determination and discrimination. Analytics involves algorithms. In many cases, we don't know the assumptions embodied in them nor do we know whether the data used for analysis is complete and up-to-date. There are often so many instructions in equations, even those who build them don't know what they do. When you put this into, for example, a law enforcement or predictive policing context, the risks of discriminatory predictive analysis are alarming.

Sharon: ***The UK's position around open data is to set up a transparency board to keep the governance around open data, big data and its handling transparent. Do you think that would create vulnerabilities or is transparency something to strive for with you?***

David: The transparency board was absorbed into Data Steering Group late last year. My understanding is that it promotes open data by ensuring that the UK open data program aligns with the government's strategic goals. It is an open data champion. In that sense, its transparency role is tangential to a privacy or security transparency role. For example, I haven't seen any published material about its views on de-identification of released data sets.

Sharon: ***How would you like to see "privacy by design" being implemented in Victoria? My understanding from hearing you speak in the past is that you had quite a strong view about adopting that approach for business, but how would you like to see it being implemented in Victoria?***

David: We are the only privacy office in Australia that has adopted Privacy by Design (PbD) as a policy. It has been welcomed in Victoria and is being implemented by many agencies. It is a methodology that helps them to build privacy into new information initiatives from the outset. PbD provides policy development and system architects with an internationally accepted approach to privacy implementation. One of the main PbD tools is a Privacy Impact Statement (PIA). A PIA is designed to assess privacy risks and encourage risk mitigation strategies. We are now seeing PIAs being undertaken by most major public sector information projects. This is a fundamental step towards implementing PbD and is a welcome development.

Sharon: ***What are the specific challenges facing law firms around privacy?***

David: Most lawyers do not know how to work positively *with* privacy or security. They take a black letter law approach to interpreting the privacy principles, forgetting that the objects of the law, including the need to facilitate the free flow of information, are taken into account. Both privacy and security involve risk assessment — lawyers understand legal risk but do not always understand information risks holistically and almost never understand policy risks.

Sharon: ***Tell us about the privacy principles that impact on CCTV and surveillance and your view on safeguarding this information?***

David: The development of surveillance technologies raises many privacy concerns. Some reflect out-of-date technology. With earlier versions of CCTV systems, individuals may not have been identifiable because the technology was so primitive — all you could do was see there was a human being there. That is no longer the case, but signage and notification has not kept up with the technology. In the meantime, the internet of things has developed and devices like drones are commonly available.

There are real privacy and security issues associated with these. For example, many agricultural equipment manufacturers include sophisticated sensors in their machinery. These transmit information about their use, including information about crop yields, soil moisture levels and patterns of use back to the manufacturer. The sensors cannot be turned off and the manufacturers sell the information onwards. These practices are almost entirely unregulated.

We rarely consider the security of surveillance data. How securely is the data stored? Who has access to it? How long is the data kept? A lot of CCTV footage is collected by small businesses and in many cases, they are not covered by privacy or surveillance devices laws.

Sharon: ***I was actually going to ask you about that, because you have expressed concern in the past that OAIC (Office of the Australian Information Commissioner) has no jurisdiction over companies whose turnover is less than 3 million dollars each year. Can you tell me a bit more about that yawning gap?***

David: Something like 90% of the private sector is not covered by privacy law. That represents a huge number of organisations that collect and handle personal information that are completely unregulated by privacy law. This is one of the key reasons why the EU has never accepted Australia as a jurisdiction where EU personal information can be processed. This inhibits Australia's ability to fully participate in the global information economy.

Sharon: ***Can you tell me about a time where you have personally been challenged by privacy?***

David: We decided we wanted to change our energy supplier. I terminated the supply agreement in writing. Following that, representatives of the supplier phoned frequently to entice us to stay. Each time a representative called, I was asked to answer a number of intrusive questions. When I asked why, I was told that it was to identify me. This is the only time I've responded by saying: "That's not right — and I'm the Privacy Commissioner!" We now have a new supplier.

Sharon Givoni
Principal Solicitor
Sharon Givoni Consulting
sharon@iplegal.com.au
www.sharongivoni.com.au

Photo of David Watts