LIV Government Lawyers Conference: Keynote address

Speaker: Sven Bluemmel, Information Commissioner

Date: Friday, 22 June 2018

Information access, privacy and data protection: A new approach for modern government

Good morning everyone and thank you to the Law Institute of Victoria for allowing me the opportunity to speak this morning.

I would like to start by acknowledging the Wurundjeri people of the Kulin Nations as the Traditional Custodians of the land on which we are meeting today. I would also like to pay my respects to their Elders, past and present, and the Elders from other communities who may be here with us 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 an Information Commissioner! 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.

I must add, while I may be Victoria's first Information Commissioner, I am certainly not alone in my role. I am supported by two Deputy Commissioners. Acting in the role of Public Access Deputy Commissioner is Joanne Kummrow, who is responsible for Freedom of Information. Rachel Dixon is the Privacy and Data Protection Deputy Commissioner and responsible for privacy and data protection. Together, Jo, Rachel and I are supported by about 50 staff.

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. OVIC combines the functions of the previous Office of the Commissioner for Privacy and Data Protection and the Office of the Freedom of Information Commissioner.

The establishment of OVIC signals a new direction for engagement with public sector agencies and entities to assist them in information management issues and to help drive systemic and cultural change.

To quote from the second reading speech of the FOI Act amending Bill:

> *The creation of this new office will provide more proactive and integrated FOI, privacy and data protection leadership in Victoria, particularly by driving the cultural shifts necessary to improve the way government manages and provides access to information.*

Over the past 9 months, I have been spending a significant amount of my time engaging with stakeholders to promote and drive cultural change in the administration of our legislation.

Today, I would like to provide you with an update on the three functions of my office and comment on the recent changes we have seen in the legal landscape, including the enforcement of the EU's General Data Protection Regulation and a host of information sharing reforms in Victoria.

Information Rights in Modern Society

I wanted to begin by touching on some of the more philosophical theories underpinning our information rights, including our rights to information access and information privacy, as we know them today.

Information is the lifeblood of society. The ability to exercise control over our personal information is essential to the development of one's identity and sense of self. Given the reality that our lives are increasingly being lived out in the digital sphere and the permanence of our online activity, information privacy is arguably becoming more important than ever before.

It is tempting to see information rights as a first world luxury. However, a similar argument applies to many rights that we hold dear as being hallmarks of a free and fair modern society. This includes rights to freedom of expression and religion, the right to a fair trial, equality before the law and protection from torture or inhuman treatment. I don't think that anybody would seriously argue that these rights are not important.

Being government lawyers, I'm sure that you are all aware that all of these rights are enshrined in the Victorian Charter of Human Rights and Responsibilities. A further right enshrined in the Charter is the right to privacy. The protections afforded under the Privacy and Data Protection Act are integral to realising the right to privacy. I do not think it an understatement to say that information rights are as important to an individual's ability to participate meaningfully in society as are the right to freedom of expression or, for adult citizens, the right to vote.

All of this is a recognition that information rights matter to us as individuals and as a society. That is not to say that these rights are unconditional or absolute. But we all know that an impulsive tweet or a regrettable photo on social media can have lasting effects on a person's reputation and future opportunities.

I won't ask for a show of hands, but those in the room who, like me, are over 45, are probably grateful that our own teenage years occurred at a time before social media.

An Overview of Information Rights in Victoria

What, then, is the current state of information rights in Victoria? To answer this question, I will turn to each of the three domains of information rights under my office's remit.

Starting first with information privacy. Like most, but not all, Australian jurisdictions, Victoria has legislation that requires State and local government agencies to adhere to a set of Information Privacy Principles, or IPPs, when collecting, storing, using, disclosing or destroying personal information about individuals. In our case, these obligations are enshrined in the Privacy and Data Protection Act.

This is complemented by Commonwealth legislation that imposes similar obligations on Commonwealth government agencies and much of the private sector throughout Australia. Importantly, this legislation allows for an independent body to hear and resolve disputes about interferences with a person's privacy. In Victoria, my office fulfils that function.

In relation to data security, the Privacy and Data Protection Act establishes the Victorian Protective Data Security Framework. That framework requires agencies to adhere to 18 Victorian Protective Data Security Standards that have been endorsed by the Special Minister of State.

Finally, the Freedom of Information Act provides a public right of access to documents held by State government agencies, statutory authorities and other public bodies. This is not an absolute right but is subject to a number of exemptions to account for those situations where, in the opinion of Parliament, the public interest in transparency is outweighed by other valid interests such as the protection of personal privacy. Again, the legislation allows for my office to undertake independent reviews of agency decisions as to whether or not particular documents are exempt from disclosure.

Information driving modern government

Let us now look at practice. In carrying out their democratic and statutory functions, governments collect, handle, use and store vast quantities of personal data about their citizens. This is particularly clear from our increasingly digital engagement with government. In a public sector context, much of the most valuable data to which government has access contains personal information about individuals.

Used and shared appropriately, personal information can enable governments to make informed decisions and provide better policy and service responses to the issues of the day. These objectives must be achieved while ensuring that Victorians are able to enjoy their information rights. This is precisely where OVIC's mandate lies, in the administration of the FOI Act and Privacy and Data Protection Act, to protect the information rights of the public. This is why we exist.

Freedom of Information

As I mentioned earlier, today I would like to provide you with a snapshot of the some of my key observations and priorities for each of the functions of my office, while hopefully providing you with some insights into the common issues in information law, that you can take back to your roles. I will begin with FOI.

Victoria was the first Australian state to enact FOI legislation. The Victorian Act closely followed the enactment of a Commonwealth FOI Act. Before the Commonwealth and State FOI Acts where introduced, the various governments of Australia had no general legislative obligation to release information to the public.

In essence, some of the justifications for FOI laws are:

First, that transparency is essential to political accountability, and to discouraging corruption and other forms of wrongdoing.

Second, that the publication or release of information about the structure, organisation and workings of public sector bodies promotes increased participation in decision making.

And third, that individuals should be able to access their personal records to assure themselves that they are accurate and complete, and to seek their amendment if they are not.

Unlike elsewhere in Australia, Victoria's FOI Act has not undergone a major overhaul since its enactment, although it has seen incremental changes over the years. In that time, FOI in Victoria has evolved in a way that means we now face some critical challenges.

Victoria receives the highest number of FOI requests of all the States and territories of Australia. In 1984-85, there were 4,702 FOI requests,[1] compared with 36,219 in 2016-17,[2] which itself was a 5% increase on the previous year. Anecdotally, it seems that requests are also increasing in scale and complexity.

This is at least in part due to the fact that Victoria has what we refer to as a 'pull model' for FOI rather than a 'push model.' A push model is one in which information is proactively pushed out. States that have a push model proactively and routinely release information to the public, independently from FOI-based information access and disclosure regimes, which are largely a reactive. Victoria does not have this push approach; however, my office is increasingly promoting and supporting the release of information outside of FOI, wherever possible. I touch more on this in a moment.

Amendments to the FOI Act that came into effect on 1 September 2017, also reduced the maximum timeframe for responding to an FOI request from 45 to 30 days, and introduced new third party

[1] VAGO Audit Report, *Freedom of Information*, 2012, page 7.
[2] FOI Commissioner Annual Report 2016-17, page 42.

consultation requirements for agencies when considering whether certain exemptions apply. While many agencies have adapted their processes to respond to these changes, early indications are that the requirement to consult third parties is adversely affecting the timeliness of agency decisions.

More generally, there has also been criticism of the way the FOI Act in Victoria is administered. The Victorian Auditor-General, in the 2012 audit report on *Freedom of Information*, stated that:

"Since FOI legislation was introduced 30 years ago, Victoria has gone from being at the forefront of FOI law and administration to one of the least progressive jurisdictions in Australia."

The Auditor-General pointed to "the Victorian public sector's systemic failure" to support the public's "right to timely, comprehensive and accurate information."

While considerable work has been done in response to that report – particularly by the agencies that were subject to the audit – there remains the perception, not without justification, that Victoria is lagging when it comes to FOI.

Recent media reporting has picked up on declining release-in-full rates, increasing deny-in-full rates, agencies adopting an overly technical approach to the interpretation of the Act, and external review decisions that appear to be out of step with other jurisdictions. That perception undermines the community's level of trust and engagement with the public sector through government openness and transparency.

My vision for FOI in Victoria is to ensure that government agencies, through working with OVIC, routinely provide improved outcomes for applicants under the FOI Act in timeliness, convenience and informality. More information will be proactively released, other information will be released upon informal request and the FOI process will be used as a last resort.

I will now highlight some of the key initiatives we will pursue to achieve these objectives.

Facilitating information release

OVIC encourages agencies to identify ways to provide access to information, without the need for individuals to make a formal request under the FOI Act. We will be encouraging public sector leaders to authorise their staff to approach requests for information with the mindset of *can we facilitate access without going through the FOI process?*

Where a matter does go through FOI, OVIC will be supporting agencies to adopt a more flexible, less technical approach.

We want to develop a culture where it gets easier and easier to do the right thing in providing access to information held by government. We want to encourage agencies to consider more informal mechanisms for the release of information held by the public sector and in turn, discourage overly-technical readings of the FOI Act which are often contrary to the desired outcome of FOI, which is to improve government transparency and accountability.

My impression so far is that while many agencies are approaching the FOI Act with a view to releasing information reasonably, others are still devoting considerable effort to finding loopholes and adopting technical approaches to avoid their obligations under the FOI Act or delay reviews by my office.

There will be FOI requests that are complex; where the stakes are high; where the public interest considerations are finely balanced. The FOI access regime and the external review process are designed for such matters.

However, the vast majority of FOI requests continue to be made by members of the public, for access to their own information. While these types of requests are not without their complexity, the statistics demonstrate that there are considerable gains to be made by agencies proactively identifying opportunities for 'routine' or 'administrative' release regimes.

My experience has been that this will improve outcomes for the community, as intended by the FOI Act and the Parliament, and enable agencies to better focus their FOI resources.

Proactive disclosure

Of course, administrative access schemes are reactive. So, as another way to facilitate information access outside the formal FOI process, OVIC will be supporting *proactive* disclosure regimes, as an effective way to fulfil the object of the FOI Act.

While the proactive and informal release of information will depend on agencies to reconsider their approach to access to information and open government, I am confident that proactive disclosure will lead to positive outcomes.

Of course, providing the public with full and open access to public sector information depends on agencies first understanding and being able to properly manage the information they hold.

The Victorian Auditor-General's 2015 report, *Access to Public Sector Information*, expressed doubt that many agencies had reached a level of maturity in information management to properly facilitate access to public sector information.

OVIC has been working with agencies to address this in a number of ways, including by promoting the use of Information Asset Registers as an important tool for identifying, valuing, and managing risks to an agency's information assets

Development of Professional Standards

Another of my key priorities is the development of and consultation on new Professional Standards under Part IB of the FOI Act.

The purpose of Professional Standards is to ensure greater public access to government held information, by providing agencies with clarity, and making them accountable for acting consistently with the pro-disclosure object of the FOI Act.

Principal officers will be directly responsible for ensuring that all of their staff, not just FOI officers and units, are aware of and comply with the Professional Standards. This significant amendment recognises that access to information held by Victorian agencies is a shared responsibility.

The Standards could also deal with matters such as appropriately resourcing the FOI function, and professional development for FOI officers and decision makers.

We look forward to consulting with agencies about the issues to be addressed in the Professional Standards.

Training, education and awareness

Lastly, one of our key initiatives is to provide regular quality training and education offerings to agency staff. Our training will continue to be directed not only to assisting agencies with processing FOI requests, but also providing meaningful guidance on how to administer the FOI Act consistently with its object. Our training will reflect the professionalism required of FOI practitioners and promote best practice.

I am pleased to say that from 1 July this year, all of our training will be offered to agencies free of charge.

Other initiatives include providing detailed guidance for agencies on administrative release and proactive disclosure, and developing a cross-sector 'community of practice' where FOI practitioners can come together to share knowledge and be recognised for excellence.

In the FOI space, OVIC too needs to work smarter to meet increasing demands on our office. We have seen a 40% increase in the number of applications for review and complaints to our office in 2016-17 over the last three years. This has continued into the current financial year.

Our office is implementing a range of measures to improve the timeliness and efficacy of our external review and complaints process. These measures include a greater focus on informal resolution and early finalisation of review and complaint matters through direct and prompt engagement between OVIC, applicants and agencies.

Privacy

I will now move on to take a look at some of the key developments in the information privacy space, which my office regulates under the Privacy and Data Protection Act.

Undoubtedly, privacy is 'having a moment' in 2018. Public awareness of privacy has gained momentum recently, with the news of the Cambridge Analytica data breach coupled with the enforcement of the EU's General Data Protection Regulation, or GDPR, dominating our newsfeeds.

Something that the Cambridge Analytica data breach highlighted is the notion that privacy is no longer a one-to-one transaction, or a matter of specific, independent choice, as a consumer. You may have come across an opinion piece written by Waleed Aly earlier this year, commenting on this very shift in the privacy paradigm – that individuals giving away their personal data to access services online are no longer consumers, rather, they are the product.

Aly writes:

"*Viewed this way, privacy becomes something new. Not so much a thing that's your own, and more a thing in which we all have a stake. In the networked world of Facebook, your lack of privacy is everyone else's problem.*"

I like to think of privacy as a public good, similar to clean air or safe drinking water. If you think about privacy as a public good, we *all* suffer when some of us choose to allow broad access to our personal information, just as we *all* suffer if some of us choose to pollute the water supply. We need to shift the way we think about privacy from a purely *individualistic* or transactional mind-set, to one that is more collective and long-term.

Given the rise of the connected economy, largely fuelled by exchange and pooling of personal data, a question we all must ask ourselves is – *how do we keep the law in time with rapid technological change, and in turn, the increasing commodification of personal data?* The law reform process tends to move at a slower pace than technological advancements and data-driven innovation.

One answer can be found in the legislative approach taken by the EU, in the General Data Protection Regulation or GDPR. This sets a blueprint for modern privacy law in many ways, responding to the use of personal data for competitive advantage. The principles relating to the processing of personal data under the GDPR, reflect the founding principles of privacy law – collection limitation, purpose specification, use limitation, accountability and so on.

Yet, the GDPR also prescribes exactly the mandatory privacy and data security obligations of data controllers and data processors. The key reforms from our perspective, are the obligations for transparency, accountability and data protection by design and default codified within the GDPR.

The GDPR mandates good privacy governance and practice, placing obligations on entities to demonstrate compliance; ensure transparency in all privacy communications, primarily through the requirements use of clear and plain language; and build privacy into their everyday business operation. The GDPR is also why all of us have received so many privacy notices and new terms and conditions for various apps and services over the last few months. It is also why Australians' Facebook data will now be hosted in the US, instead of Ireland.

Most of us will be familiar with the concept of the 'social contract,' which says that the State's authority and legitimacy comes from a tacit understanding between the people and government – citizens agree to give up some of their freedoms in order for government to protect their other rights.

When requiring individuals to supply personal information, government has a responsibility to protect it. Without a guarantee of privacy protection, government loses its social license to use people's information, and the public's trust diminishes.

In addition to building the public's trust and confidence in government, the way that organisations manage their privacy governance has an impact on their reputation and, in some cases, their finances, as the costs of managing privacy breaches and retrofitting systems and processes to incorporate privacy measures can be significant.

Good privacy governance in practice means taking proactive steps to manage privacy, which is reflected in the requirement to take a data protection by design and default approach to practices under the GDPR, coupled with the statutory requirements to undertake data protection impact assessments. These obligations for data controllers and data processors under the GDPR creates an overall healthy privacy culture – which is what we are all aspiring to.

Last year, my office hosted a public forum on the GDPR, framed in terms of key lessons for the Victorian public sector. Some of the themes raised at our public forum included the enhanced, actionable rights for individuals provided for under the GDPR and the strengthened requirements for informed consent under the GDPR. We have continued to explore these themes in our GDPR guidance, published on our website last month.

The approach of the GDPR has prompted law reform across a number of jurisdictions. There are certainly key elements of the GDPR reflected in recent reforms at the Commonwealth level. In February this year the Commonwealth Notifiable Data Breaches Scheme came into effect – which also applies to the Victoria public sector to the extent that an eligible data breach involves Tax File Number information.

Two key pieces of legislation recently passed in Victoria, the Victorian Data Sharing Act and the Service Victoria Act both include mandatory data breach notification requirements to OVIC. These reforms were the product of early and positive engagement with our office.

Similarly, at the Commonwealth level, the Australian Government Agencies Privacy Code also comes into effect on 1 July this year, which reflects core elements of the GDPR's focus on overall good privacy governance, including executive oversight of privacy practices.

Information sharing

Let us now look specifically at information sharing. Organisations, including government agencies, are grappling with increasing demand to share information, the effective de-identification of data, and giving effect to the privacy obligations that carry through to the public sector's contracted service providers.

A challenge for any organisation, whether public or private, is knowing how to reap the social and economic benefits of data while establishing and maintaining strong privacy and security protections. Some of the most recent challenges in information sharing are not necessarily technology-related. Of course, the legal and ethical challenges underpinning the use of big data, AI and the Internet of Things, to name a few, remain.

Yet, alongside these technological changes, as government lawyers, you will be well-placed to assist agencies to navigate some of the most immediate challenges facing the need for lawful, careful and timely information sharing in the public sector, as these are questions primarily of statutory interpretation and risk management.

The legal landscape has changed somewhat over the past two to three years, with the introduction in Victoria of the new family violence information sharing scheme; the forthcoming child information sharing scheme; and the implementation of the Victorian Data Sharing Act – establishing the role of the Chief Data Officer, who leads the Victorian Centre for Data Insights.

I want to highlight that it is certainly not within the spirit of these reforms to displace or ignore privacy. The use of data for better service delivery and policy design in the Victorian public sector does not have to come at the expense of privacy. Rather, these reforms have been designed to reconcile the need for information sharing in certain circumstances with the protection of privacy.

I would encourage all of you rethink how you see the role of privacy law in an information sharing context. There is a lingering misconception that privacy law is a barrier to information sharing. However, this is generally not the case.

The Privacy and Data Protection Act contains a number of mechanisms to facilitate information sharing in certain cases. These include the exceptions under Information Privacy Principle 2.1, as well as the flexibility mechanisms under the Privacy and Data Protection Act, that permit departures from the IPPs where there is a substantial public interest in doing so. This signals to the VPS and the public that privacy law is not intended to stand in the way of other legitimate public interests.

When faced with an information sharing question, my initial advice to you would be, in the words of Douglas Adams – don't panic! Your starting point should be to carefully check and interpret existing legal authorities to share information.

For example, the family violence information scheme has been designed to operate in conjunction with existing legal authorities to share information.

It is important to know and interpret your authority for sharing information. If that authority is indeed under Information Privacy Principle 2.1, be mindful of the interplay between the notice requirements of IPP 1, that place an obligation on agencies to tell individuals why they are collecting their personal information and ensure that this notice is consistent with the intended uses of the information – including sharing with others.

Next, it is important to map the relevant information flows and apply the requisite privacy and data security protections required, proportionate to the level of risk associated with the information. While some recent information sharing reforms provide the clear legal authority to share information for a specific purpose, this should not displace the obligations under the IPPs entirely.

In practice, the Privacy and Data Protection Act will only be displaced to the extent that a provision of another Act relating to an Information Privacy Principle is inconsistent with the Privacy and Data Protection Act. This will require you to navigate the obligations under enabling legislation and the privacy obligations under the Privacy and Data Protection Act together.

Actively committing to share information responsibility can help to increase public trust in agencies. People need to feel secure in the knowledge that government is handling their information appropriately and lawfully. That confidence, in turn, builds the social licence given to government to deal with individuals' data as the public has trust in the public sector's stewardship of their personal information.

One way to demonstrate a commitment to share information responsibility is to conduct a Privacy Impact Assessment, or PIA, early in the development stages of any new initiative. This process will require agencies to identify their legal authority to share information and map information flows accordingly.

However, I would stress that conducting a PIA is not a tick and flick exercise and any PIAs should be revisited periodically, to account for changes in programs and the way information is used. OVIC also encourages agencies to publish PIAs, or make publicly available a summary of the key privacy concerns raised in a PIA, as a measure to build public trust in the use of their personal information. Our office is always available to assist organisations navigate their privacy obligations in an information sharing context.

On that note, when facing challenges in meeting statutory obligations or planning projects that have FOI, privacy or data protection implication, I would encourage you to consult with us **at an early stage**. We are here to help and engaging with us early will allow us to provide you with the guidance to meet your objectives as well as to ensure strong privacy and security protections in any proposed initiative.

While OVIC, as an independent regulator, needs to maintain its independence from being involved in the particular design of projects or initiatives, we are committed to providing practical guidance and expert knowledge to agencies, to assist them in facilitating their information-related projects and obligations.

Practicing in the area of information rights: Be aware of differing perspectives

On the topic of information sharing, and information rights more broadly, I think it is essential that practitioners continue to gain an understanding of the different needs and perspectives of others, to allow you to better advise your clients or agencies.

We can no longer assume that the world sees the use of data in the same way as we do. While one person may have no reservations about government sharing their information, and indeed, they may even expect their information to be shared in order to access streamlined government services, another person may have a totally different perspective when it comes to information being shared about them.

For example, in a family violence context, for a victim-survivor trying to escape a perpetrator, the privacy and the security of their personal information will be essential to their safety. The family violence information sharing scheme takes a victim-centric approach to information sharing, to ensure that these considerations are taken into account before information is shared, acknowledging that their privacy (and the privacy of their family) will be a primary concern.

These reforms are designed to realign the power imbalance between victim-survivors and perpetrators in a family violence context and prevent perpetrators accessing information about vulnerable individuals. To a victim-survivor of family violence seeking to escape their perpetrator, information privacy will be fundamental to their own safety and in some cases, their life.

So, as you are interpreting and applying the legislation that underpins the information sharing agenda of today, or even designing or advising on new information sharing initiatives, it is essential to consider the viewpoint of those most acutely impacted by the reality of information sharing.

Similarly, in an FOI context, it is important to note while you as government lawyers will be working to help your agencies and client meet their FOI obligations, not everyone works for the government. For example, the motivations of investigative journalists, interest groups and private enterprise to use the FOI process may be fundamentally different to, but no less valid than, those of government lawyers.

Data protection

The third function of my office that I would like to talk to you about today is data protection. I have already mentioned that the Privacy and Data Protection Act establishes the Victorian Protective Data Security Framework that requires agencies to adhere to 18 Standards that have been Ministerially endorsed.

Our aim for data protection is to work to facilitate the ongoing improvement of the data security practices of Victorian government agencies, rather than striving for perfection. The nature of data protection and the constantly evolving threat environment means that encouraging agencies to take a risk based approach to data security will support businesses achieving their objectives, in a manner commensurate with their resources. And also note that I refer to improving *practice*, not just systems or technology.

Good data security is more than just ICT. You may have the most secure software and technology in place to protect your information, however, if there aren't appropriate overall controls in place to limit access to that information, such as physical and personnel security, then the information may still be compromised.

I would like to highlight that from a practical point of view, while privacy and security are different concepts they are inextricably linked – you can't expect to maintain overall good privacy governance if your data security practices are poor.

Beginning in August this year, and every two years thereafter, agencies will need to provide a high level Protective Data Security Plan to my office, together with an attestation on behalf of the head of the agency about the agency's protective data security activities.

I want to stress that the purpose of the Plans is not to serve as a measure of who is the most 'compliant' with their data security obligations. Rather, it is a matter of constant improvement. Our data protection team is currently working to assist VPS organisations to demonstrate their adoption of the Framework and Standards.

The Standards have been drafted to represent best practice in data security, taking into account the policy and operational responsibilities of the Victorian government and are reflective of national and international approaches to security. So, if your agency or your client has already committed to best practice for data security, it is likely that they will not have to do much extra to meet their data security obligations under Part 4 of the Privacy and Data Protection Act. The Framework and the Standards are not technically prescriptive and cover a range of security domains, including physical security, ICT security, information security and personnel security, underpinned by good governance.

My office's guidance material and reporting requirements placed on agencies will only lead to meaningful and positive change if those materials are respected as having been built on a solid foundation of recognising agency business realities. To ensure that this is the case, we need to talk to agencies. At all levels of their business. OVIC's data protection team has been doing exactly that.

OVIC's regulatory approach

Not so long ago, some of you may recall that I was presenting my vision for OVIC. That was to be a regulator that engages constructively with agencies to achieve the legislative outcomes that have been entrusted to us by Parliament – while maintaining our independence and impartiality.

I am pleased to report that in just 9 short months, my office has been open to consultation, both proactive and reactive, from agencies seeking to enhance their FOI, privacy or data protection practices or implement new initiatives.

I want to ensure that agency practices in privacy, data protection and information access are consistently improving, ensuring that Victoria's approach to handling information is as robust as possible. The way I foresee doing this is to make it as easy as possible for agencies to do the right thing.

OVIC welcomes the opportunity to work with Victorian agencies in a positive and collaborative manner and it has been encouraging to see the agencies that we have worked with regard us as an enabler for their objectives, rather than as a regulator who delights in punishing them when they do something wrong. In short, we are here to help.

Concluding remarks

Let me finish by saying that it has been a pleasure to come here and talk to you all today. I want to conclude by leaving you with three key messages.

First, don't perceive privacy as a barrier to information sharing.

Second, be constantly aware of other people's perspectives and needs and don't assume that everyone sees the world as you do.

Third, please engage with us early on matters that have an information policy dimension. Our doors are open and talking to us in the early stages of any new initiative will allow us to support you to achieve your policy objectives while ensuring strong privacy and data security protections.

We hold quarterly public forums, deliver free training, host annual events such as Privacy Awareness Week and Right to Know Day and publish plenty of guidance material on our website. Our brand new website, at ovic.vic.gov.au, should be live in a few weeks and has all of this and more. If you sign up to OVIC's Twitter feed, you will be kept up to date.

We're reaching out, so look us up and get in touch.

Thank you.