

---

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

**Speaker:** Sven Bluemmel, Information Commissioner

**Date:** Tuesday, 27 February 2018

### Introduction

On behalf of Sally, Rachel and myself, I thank the VGSO for the opportunity to speak with you this afternoon.

I would like to start by acknowledging the traditional lands of the Wurundjeri people on which we are meeting today.

I wish to acknowledge them as the Traditional Owners of this land. I would also like to pay my respects to their Elders, past and present, and the Elders from other communities who may be here today.

I am delighted to be here to speak with you as Victoria's inaugural Information Commissioner.

### Brief history

It is interesting to reflect on OVIC's short five month history when compared to the VGSO's more than 165 year history of providing legal advice to successive Victorian governments, Ministers and agencies.

In its early days of establishment, I am sure the VGSO, or the Crown Solicitor as it was previously known, looked to the future with an ambitious agenda to serve government and the public. While many years separate the establishment of OVIC with the VGSO, their roles and vision are likely to share some common elements.

There is, however, at least one key difference. And that is, that OVIC is not here to serve government, but rather to ensure that government's collection, use and disclosure of information is done in a way that serves the community, as envisaged by Parliament.

This may occasionally lead to disagreements between government and OVIC, but that is all part and parcel of being an independent regulator. It is not something to be avoided, but something to be managed constructively.

OVIC has combined oversight of Freedom of Information, privacy, and data protection. It combines the functions of the previous Office of the Commissioner for Privacy and Data Protection and the Office of the Freedom of Information Commissioner. Rachel, Sally and I are supported by about 50 OVIC staff.

OVIC's establishment signals a new direction for engagement with public sector agencies and entities to assist them in information management and access issues and to drive positive systemic and cultural change. It also means we can build a consistent regulatory approach across all three areas of FOI, privacy and data protection. This will not always be straightforward, as there can be a degree of tension between these areas.

However, I see the establishment of OVIC as an opportunity to acknowledge and deal with those tensions, allowing us to provide clear and consistent guidance to the Victorian State and local public sector. Having those elements administered by a single regulator also reflects the reality that all aspects of information management can have very real impacts on the lives of individual citizens.

As Victoria's inaugural Information Commissioner, let me turn to my vision for OVIC and what our success will look like.

## **My vision**

Access by individuals to information held by government and government's handling and protection of personal and sensitive data about individuals are key elements of modern government and underpin the fundamental aspect of the relationship between citizens and their governments.

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 pertinent in our increasingly digital engagement with government.

The physical service counter equipped with staff and paper is being replaced by online portals with the ability to collect, use and share personal information at the touch of a button.

There is immense value in the personal information held by government and the private sector alike. In this morning's press, Australian Competition and Consumer Commission chairman Rod Sims said that consumers should *not* think of Facebook or Google as free services, because there is a cost to giving the tech giants so much personal data.

To this end, the ACCC inquiry into the impact of major digital platforms will investigate whether users are being misled about that cost. Mr Sims went on to say "there is nothing free in this world. So if someone is providing you something for free you need to think 'how is that so?'"

You can tell that I am *not* a millennial because I just referred to "reading this morning's press" rather than getting my news on Facebook. And it is often asserted that younger generations are much less concerned about privacy, or even not significantly concerned about privacy at all. "Privacy is dead – got over it".

But in my view, that has always been an unfair oversimplification. I believe that younger generations are very savvy about their information rights, even if that savvy manifests itself in ways that are quite different to previous generations. Recent surveys both in Australia and abroad bear this out. One of these surveys distinguished between "older Millennials" and "younger Millennials". I did find that a little depressing.

In the public sector context, much of the most valuable data to which government has access contains personal information about individuals. Used appropriately, this information enables government agencies to make informed decisions and provide better policy and service responses to the issues of the day.

But government and personal data is not a one way street.

In order for government to legitimately collect and use the personal information of its citizens, it needs to ensure that it maintains a trusted relationship with its citizens who are assured that their personal information will not be misused or shared unlawfully. Without trust, the social compact that effectively exists between society and government is severely weakened.

It follows then that citizens have a general, if not unfettered, right to access information held by government, and should be entitled to trust that government is only collecting personal information necessary for its functions. Where it does collect such information, citizens have a right to expect that government securely stores this data and that any use of the data is lawful and in line with reasonable community expectations.

This is where legislation such as the *Privacy and Data Protection Act* and the *Freedom of Information Act* come in.

Each provides a legal framework for the way in which:

- government collects, uses, discloses and stores personal and sensitive data, and
- how an individual can seek access to information held by government and ensure any personal information held about the individual is accurate.

Such 'information rights' are increasingly important in order that individuals can meaningfully participate in society and understand their relationship with their government.

My office recently commenced a process of strategic and operational planning for the years ahead. As part of that process, I put the following deliberately provocative question to staff: *Why do we need to govern how the public sector collects, stores, uses, discloses and secures information?*

One of the answers that came back was, in part, that in the information age, control over information *is essential to the establishment of individual identity*. We are not talking there about a proof of identity process to access a product or service. Instead, we are talking about what it means to be human in the digital age.

Upholding the privacy of an individual's personal information is paramount for a number of important reasons:

1. Privacy is recognised as a human right, internationally under Article 17 of the International Covenant on Civil and Political Rights. It is also enshrined in s 13 of the Victorian *Charter of Human Rights and Responsibilities*.
2. There are significant economic and social benefits in establishing strong relationships between government and the public based on trust and transparency.
3. 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.

A challenge for any organisation, whether public or private, is knowing how to reap the social and economic benefits of all of this information while establishing strong privacy and security protections.

Technology further enhances this challenge. It creates uncertainties around how personal information is to be handled in accordance with privacy laws. This is evident through big data, Internet of Things devices, artificial intelligence and blockchain technology.

I will *not* ask for a show of hands as to which of us actually proclaim to understand blockchain, primarily to prevent self-incrimination. But when you have the government of Venezuela launching its own crypto currency based on distributed ledger technology and backed, no less, by that country's oil reserves, you can be sure that the world is changing.

Alongside the technological issues, experience tells us that organisations are also 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.

OVIC is working towards facilitating closer working relationships with agencies to assist them in meeting their privacy obligations and assisting them to achieve their information sharing objectives in a privacy-enhancing way.

We want agencies to utilise us in planning their projects and building in privacy protections, and to seek our advice and assistance, where required. While we will always need to maintain our independence as a regulator from particular projects or initiatives, we will always strive to provide practical advice to agencies.

## **OVIC as regulator**

I now turn to how OVIC will go about its work and what agencies can expect from our approach.

As I have already said, my vision for OVIC is to be a regulator that engages constructively with agencies to achieve the legislative outcomes that have been entrusted to us by Parliament – while also maintaining our independence and impartiality.

I want to ensure that agency practices in privacy, data protection and information access and sharing 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. Key to us being able to achieve this will be continuing the conversation. Sally, Rachel and I need to understand the environment that agencies operate in, the challenges they face, and the areas where more guidance is needed.

While a regulatory body has an important statutory role to play, it's my intention that our engagement with agencies is focussed on support, guidance, and constructive feedback. During OVIC's first six months, agencies have sought our views on early drafts of new legislation regarding privacy impacts, and agencies are self-reporting suspected data breaches to our Office to seek advice on how to respond.

Experience continues to show that trying to sweep such things under the carpet merely delays the inevitable and usually makes it worse.

The approach we want to take is to work with agencies and assist them in developing their own capability. It has been great 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 catching them out when they 'do something wrong'.

If agencies are open about their issues, we will work with them to help find a solution. However, this regulatory approach places some demands on agencies about how they deal with us.

There will certainly be disagreement from time to time between agencies and OVIC about whether a particular document is exempt from disclosure under FOI, whether a practice by an agency amounts to an interference with an individual's privacy or whether an agency is meeting its particular obligations under the Victorian Protective Data Security Framework. This situation is not to be feared.

As long as agencies respect OVIC's legislative remit and are open, constructive and responsive in their dealings with us, we will make allowance for the challenges you will face from time to time in .

However, if we encounter concealment, delaying tactics, and the use of technical arguments to defend the indefensible – we will use our statutory powers to call out these practices for what they are.

If you are unsure how we may respond to how your organisation plans to deal with a certain issue – don't send us a letter in a month's time. Ring us up today and talk it through with us.

## Closing

In closing, I look forward to working with all of you to achieve the important legislative reforms across the Victorian Public Sector that were envisaged at the inception of OVIC.

OVIC has a lot to do, but I know that my colleagues and I are up for the challenge. We are focussed on using our substantial legislative remit and powers to shape the best possible future for information access, privacy and data protection in Victoria.

Thank you.