SPEAKING POINTS

|  |  |
| --- | --- |
| **Event title:** | Information Rights in Victoria – What you and your clients need to knowVictorian Society for Computers and the Law |
| **Speaker:** | Sven Bluemmel  |
| **Event date:** | Thursday 6 May 2021  |

Introduction

This presentation will cover five topics, including:

* a brief overview of freedom of information, privacy and information security law in Victoria;
* how COVID-19 has impacted organisations’ obligations regarding the Freedom of Information Act and the Privacy and Data Protection Act, including through COVID omnibus legislation;
* the privacy impacts of working remotely;
* the importance of government earning our trust in how it handles our information and why this trust was so important in the State’s response to COVID-19; and
* views on the Privacy Act review.

Who we are – The Office of the Victorian Information Commissioner

Before I get into the topics I just outlined, I wanted to briefly talk about who OVIC is and what we do.

For those of you who may not be familiar with the Office of the Victorian Information Commissioner, or OVIC as we like to call it, we are an independent regulator with combined oversight of information access, information privacy, and information security.

We administer both the Privacy and Data Protection Act and the Freedom of Information Act.

Our goal is to embed in the Victorian public sector a culture that promotes fair public access to information while ensuring its proper use and protection.

We also aim to build community trust in government’s handling of information.

Brief overview of FOI, Privacy, and Information Security Law in Victoria

This brings me to the first topic I outlined: a brief overview of freedom of information, privacy and information security law in Victoria.

Freedom of information

Starting with FOI, the FOI Act enshrines several important rights and processes which promote openness, accountability and transparency in the Victorian government.

The overarching object of the FOI Act, and Parliament’s intent, is to provide access to as much government-held information as possible, quickly, and inexpensively.

By way of broad overview of the FOI Act:

* First, the Act creates a general right to request access to documents held by the Victorian government and its agencies, subject to limited exceptions and exemptions to protect essential public and private interests (such as personal privacy).
* Second, the Act requires Victorian agencies to publish certain information about themselves and their documents to help the public understand what each agency does, how it works, and the types of documents it generates and holds.
* Third, the Act provides for individuals to access their personal documents and request amendments to them if they are inaccurate or incomplete. This allows the public to make sure that the information that government holds about them is up to date, complete, and correct.
* Fourth, the Act allows for my office to undertake independent reviews of agency decisions as to whether or not particular documents are exempt from disclosure.
* Fifth, and related to my previous point, my office is also able to handle complaints about how agencies handle applicants’ FOI requests.
* Sixth, my office has the power to conduct own motion investigations into how agencies administer the FOI Act.

The FOI Act is also supported by the FOI Professional Standards, which are a legislative instrument that applies to all Victorian agencies (they do not, however, apply to Ministers).

The overall purpose of the standards is to ensure the Act is administered by agencies consistently with:

* the Act’s object – to extend as far as possible the right of the community to access information in the possession of an agency subject to the Act; and
* Parliament’s intention – that the provisions of the Act are interpreted so as to further its object and any discretions conferred by the Act are exercised as far as possible to facilitate and promote the prompt disclosure of information at the lowest reasonable cost.

The Professional Standards aim to improve communication between agencies and applicants, ensure applications are processed in a timely manner, provide clarity to certain provisions of the Act, and ensure the Act is given a modern interpretation, both in practice and process.

Privacy

Moving on to privacy, in Victoria privacy is protected in a couple of ways.

Primarily, the Victorian Privacy and Data Protection Act protects personal information held by Victorian government organisations.

Under the PDP Act, ‘personal information’ means “information or an opinion that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion…”.

However, this does not include information relating to a person’s health. Instead, health information is covered by the Victorian Health Records Act, which is administered by the Health Complaints Commissioner.

Under the PDP Act, information privacy protections are embodied in the 10 Information Privacy Principles, or, IPPs. The IPPs govern the collection, use and handling of personal information by Victorian public sector organisations, local councils and contracted service providers.

The PDP Act aims to:

* balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector;
* promote awareness of responsible personal information handling practices in the public sector; and
* promote the responsible and transparent handling of personal information in the public sector.

In addition to the PDP Act, the Commonwealth Privacy Act also protects personal information held by Australian government organisations and large private sector organisations.

Further, the European Union General Data Protection Regulation may apply to Victorian Public Sector organisations provided they satisfy certain requirements. You can visit OVIC’s website for guidance on the scope of the GDPR and considerations for Victoria.[[1]](#footnote-2)

Information Security

The PDP Act also governs information security in the Victorian Public Sector.

The PDP Act establishes the Victorian Protective Data Security Framework and the Victorian Protective Data Security Standards. Both of which are in their second iteration, following a review of the Framework and the Standards in 2017 to identify areas for improvement.

The Framework has been developed to monitor and assure the security of public sector information and information systems across the VPS.

Similarly, the Standards establish 12 high level mandatory requirements to protect Victorian public sector information across all security areas including governance, information, personnel, ICT and physical security.

The Standards:

* take into account the policy and operational responsibilities of the Victorian government;
* respect the important role that Victorian public sector organisations play in delivering services;
* reflect national and international approaches to security but are tailored to the Victorian government environment;
* focus on the security of public sector information; and
* require contracted service providers with direct or indirect access to information to adhere to the standards.

The Standards support a risk management approach that empowers government business to identify and manage its unique risks. This in turn informs good decision making, supports the achievement of business objectives, and effective information sharing whilst protecting public sector information.

How COVID-19 has impacted organisations’ obligations regarding the FOI Act and the PDP Act, including through COVID omnibus legislation

Now that I’ve provided a brief overview of the FOI Act and the PDP Act, now is a good time to shift to how COVID-19 has impacted organisations’ obligations under those pieces of legislation.

COVID-19 has changed the way that we work for over a year, which resulted in some changes and challenges with respect to the FOI Act and the PDP Act.

Highlighting that obligations don’t cease in a crisis

I will go into relevant legislative developments shortly, however first I wanted to highlight something that OVIC, our counterparts in other Australian jurisdictions, and the International Conference of Information Commissioners made clear in 2020, which was that our duty to document does not cease in a crisis, it becomes more essential.

As part of information awareness month, on 6 May 2020, the ICIC released a statement to recognise and promote sound information management practices, calling for three mandatory actions:

* Decisions must be documented;
* Records and data should be secured and preserved in all sectors; and
* The security, preservation and access to digital content should be facilitated during a shutdown.

This statement highlighted that while COVID-19 and working remotely introduced new challenges to our work, our obligations don’t pause. In fact, they become more essential.

Important decisions were, and continue to be, made by government involving significant interventions in markets, healthcare and the daily lives of billions of people.

It is essential that the basis of those decisions is thoroughly documented for government to remain accountable both now and into the future so we can learn from our actions.

Similarly, as government collects and shares more personal information for contact tracing and service delivery, it is integral that this information is secured from misuse.

Legislative changes to obligations in the FOI Act and the PDP Act

I just mentioned that our obligations don’t cease during a crisis, however some obligations did *change* over the last year.

Legislatively speaking, we saw some changes to the FOI Act and the PDP Act to try and adapt to changing work conditions to make sure we could continue to discharge our legislative obligations in a practical and efficient way.

For example, on 19 May 2020, the COVID-19 Omnibus (Emergency Measures) (Integrity Entities) Regulations were made in accordance with the COVID-19 Omnibus (Emergency Measures) Act.

These Regulations temporarily modified the FOI Act and the PDP Act to provide alternate ways to serve notices to produce or attend other than serving such notices personally. For example, service could instead be done by registered post, electronically, or providing to the person’s legal representative.

The Regulations also modified the FOI Act specifically to:

* Permit the secure electronic production of documents claimed to be exempt under section 28, 29A, 31 or 31A. Previously OVIC staff had to physically inspect these documents at the agency’s premises; and
* Provide for attendance by audio visual link or audio link with respect to the Information Commissioner’s coercive powers.

More recently, the Justice Legislation Amendment (System Enhancements and Other Matters) Act makes permanent, and in some cases extends, measures that were introduced in 2020 to allow the efficient and flexible delivery of public services.

This Act received Royal Assent on 23 March 2021, with provisions regarding the FOI Act and PDP Act commencing last week on 26 April 2021.

In terms of what this means for the FOI Act and the PDP Act, the Justice Legislation Amendment Act makes permanent those procedural requirements in the FOI Act and the PDP Act that were in the COVID-19 Omnibus Regulations I mentioned before.

This means agencies must continue to provide copies of documents claimed to be exempt under section 28, 29A, 31 or 31A of the FOI Act to my office for inspection by secure electronic means. Once my office has inspected the document, we must destroy it and let the relevant agency know accordingly.

The Justice Legislation Amendment Act also:

* extends the attendance requirements to the PDP Act, so that attendance under a notice to produce or attend under the PDP Act may be done by audio visual link or audio link – this is consistent with the temporary modifications made to the FOI Act, which are now permanent;
* allows my office to serve a compliance notice under the PDP Act via means other than personal service – for example, by post, electronically, or providing to the person’s legal representative; and
* otherwise provides that a provision in the PDP Act regarding attendance in person applies to attendance by audio link or audio visual link and similarly a provision regarding the production of documents in person applies to production of documents by secure electronic means.

These permanent legislative amendments recognise that our way of working has changed, if not forever, then for a long time into the future and we need to be able to work efficiently in line with those changed conditions.

Practical impacts on obligations under the FOI Act and the PDP Act

Practically speaking, COVID-19 has impacted how agencies have administered the FOI Act and the PDP Act on a day-to-day basis.

The most obvious impact was the need to shift to remote working, which meant a stronger reliance on technology to access ICT systems, communicate with colleagues, and coordinate activities.

What we heard from our Privacy Roundtable stakeholder group was:

* an upward trend in the number of privacy impact assessments being conducted because of new programs to facilitate remote working and COVID-19 specific programs of work such as information sharing, data compilation and ongoing relief programs;
* a significant increase in enquiries regarding the personal handling of information of individuals who have or may have COVID-19, and digitising the delivery of services;
* a need for flexibility in response times to privacy complaints with OVIC;
* an interest in more guidance from OVIC on emerging issues regarding the virus, particularly on privacy considerations associated with technology like videoconferencing.

Similarly, from our Public Access Agency Reference Group in the FOI space, we heard:

* challenges with accessing documents remotely when processing FOI requests;
* challenges with redacting documents electronically to ensure security of the redacted information;
* an overall increase in the number of FOI requests being received, particularly topical requests regarding COVID-19;
* delays in processing FOI requests;
* the importance of flexibility in administering obligations; and
* the importance of communication with stakeholders about what agencies can and cannot do in line with current conditions (for example, access to documents and timeframes).

Across both FOI and privacy, stakeholders noted challenges with staff being diverted from their usual team or business area to other functions in the agency to deal with COVID-19.

We anticipate some of these challenges will change as government returns to a more ‘normal’ working routine; with staff returning to the office more. This means more regular access to documents, IT systems, and people.

Even for staff who may remain working remotely where permissible, the fact that many agencies have established new technologies and digital tools to help them work remotely suggests that the number of enquiries and PIAs about new programs for remote working may reduce.

The privacy impacts of working remotely

The next topic I would like to speak to relates to the privacy impacts of working remotely.

Privacy impacts appear to arise in two main ways:

* Privacy risks with using new technology; and
* Privacy risks with working from home generally.

Privacy impacts of technology – collaboration tools

As I have already mentioned, remote working arrangements required us all to quickly investigate and implement new ways of working remotely to ensure business continuity insofar as possible.

For many, this transition to remote working involved the rapid investigation into, and adoption of, new technologies including collaboration tools such as videoconferencing and instant messaging tools, as well as cloud-based document creation and sharing services.

From our perspective at OVIC, this was certainly the case. We had to quickly make the shift to an online way of working, including digital communication and training tools, online redaction software, and so on.

While flexible working arrangements have been, and will likely continue to be, essential to the way we work, the ability of technologies like collaboration tools to collect, store and transmit personal information poses privacy risks.

Therefore, while technology brings with it many benefits such as increased accessibility, flexibility and efficiency, we must also consider privacy and information security before implementation such as through conducting a privacy impact assessment.

For example, many technology providers store personal information collected in the cloud or in offshore data centres.

Organisations should know where staff members’ personal information is being stored, as well as the personal information of clients and service users (if relevant) and carefully consider the privacy risks associated.

For agencies that are subject to the PDP Act, Information Privacy Principle 9 permits the transfer of personal information outside of Victoria in limited instances, such as where the recipient of the personal information is subject to a similar law, binding scheme or contract, to the IPPs under the PDP Act.

The location and storage of personal information should be considered during procurement and negotiation with vendors, if possible.

Further, some providers may have vague or lacking privacy policies. Conversely, some may have overly complicated or legalistic privacy policies or terms of use. Where possible, organisations should choose technologies that demonstrate a commitment to privacy by having clear and accessible privacy policies, and which are transparent about the way personal information is collected, used and shared with other parties.

Organisations must also remember that while some technology introduces new features and functionalities, such as recording meetings, they must still only collect the personal information they need to perform their functions. Otherwise, there is a risk of overcollection of personal information.

It’s important that you only use third-party collaboration tools or communication platforms that have been approved by your organisation, when using them for work-related purposes. OVIC recommends conducting a privacy impact assessment to identify privacy risks and how to mitigate them. Conducting assessments like this will also alert an organisation to circumstances where it should stop pursuing or using certain technology because of the unacceptable privacy risks it poses.

**Privacy impacts of working from home generally**

More generally, working remotely can pose privacy risks such as:

* People outside your organisation being able to look at your work screen or overhear work conversations – whether that be people you live with or people unknown to you if you are working from a public place.
	+ OVIC recommends avoiding working in public places if possible.
	+ Be wary of others being able to look at your work device’s screen, overhearing work-related conversations, or access any work-related hard copy information.
	+ Further, when you step away from your workspace, make sure you secure the room or lock your screen to prevent people accessing work-related information.
* Using public or unprotected WiFi networks, which can increase your risk of unauthorised persons accessing information on your computer.
	+ OVIC recommends making sure your home WiFi router has a unique password (in other words, it doesn’t use the default password on the back of the router) and make sure your devices have run any firmware or software updates. Check also to see if your WiFi connection has encryption enabled.
* Risk of phishing scams.
	+ Advice from the Victorian Government Chief Information Security Officer is that there has been a significant increase in malicious activity surrounding COVID-19.
	+ This activity includes false reports purporting to come from trusted sources such as government agencies and media outlets. Remain mindful when clicking on links and accessing digital content when working from home. If you receive a suspicious email, contact your organisation’s IT team in the first instance.

More guidance on privacy impacts of working remotely

For more guidance, visit OVIC’s website for guidance on:

* Conducting privacy impact assessments;
* Collaboration tools and privacy;
* Tips for working remotely and protecting privacy;
* COVID-19 and privacy considerations.

The importance of government earning our trust in how it handles our information and why this trust was so important in the State’s pandemic response

This brings me to the next topic for today, which is the importance of government earning our trust in how it handles our personal information and why this trust was so important in the State’s COVID-19 response.

Importance of trust in information handling generally

Broadly, government must commit to the proper handling of information in order to earn or maintain public trust in any government program or system.

On the one hand, building trust involves the responsible use of information such as only collecting necessary personal information and securing it from misuse. On the other hand, it involves openness and transparency about what government is doing so the public understands what is happening and why.

Trust in government is crucial to voluntary compliance or agreement with government policy, and it can increase the public’s tolerance of measures that seem disruptive, intrusive, or frustrating.

Conversely, distrust can result in disagreement or resistance to government policy. It can delay policy implementation and require increased investment of resources to obtain cooperation or compliance.

In the context of information handling, building trust requires organisations to commit to:

* being open and transparent when communicating with the public about how individual’s personal information will be used, disclosed, and protected; and
* implementing privacy and security frameworks to assure individuals that their information is protected, such as having:
	+ privacy and security protections entrenched in system or program designs;
	+ conducting independent privacy and security impact assessments;
	+ providing clear and transparent privacy policies to citizens; and
	+ putting in place strict parameters around the collection, use and deletion of citizens’ information.

Establishing oversight mechanisms to provide transparency and accountability to the public is also critical to maintaining public trust. For example, privacy and freedom of information regulators like OVIC are important for promoting and enforcing information rights in government programs and services.

Why this trust was important in the State’s response to COVID-19

During the COVID-19 crisis, trust in government has been more important than ever. Without trust, individuals are less likely to adhere to the strict measures that government implemented to protect the community such as stay at home orders and mask wearing mandates.

Similarly, the COVID-19 pandemic saw the government collecting and sharing more and more personal information so it could respond to the health crisis.

While privacy law permits this sharing of information, providing information for this purpose still requires trust in government to handle it securely and responsibly.

For example, privacy law does not prevent sharing and use of information where this is in the public interest. Specifically, use and disclosure of personal information is permitted where it is done to lessen or prevent a serious threat to public health. Initiatives such as well-designed contact tracing or the reasonable enforcement of physical distancing or isolation are not prevented by the PDP Act.

However, even though something may be lawful, this does not mean people want to do it, or feel comfortable doing something; government must still earn the public’s trust to do what is right.

For example, one of the key government initiatives to trace and contain COVID-19 was the introduction of a contact tracing app. For the app to be effective, individuals must feel safe to provide true and complete information to authorities.

A recent policy response published on the OECD’s website notes that contact tracing apps can provide critical information to health authorities. However, where left unchecked, extensive collection and sharing of personal information and even mass surveillance may occur.

Strong privacy and security frameworks are essential in assuring citizens that their information is protected. This means having privacy and security protections entrenched in the design of the app; conducting independent privacy and security impact assessments; providing clear and transparent privacy policies to citizens; and putting in place strict parameters around the collection, use and deletion of citizens’ information, for a start.

Maintaining public trust post COVID-19 requires governments to ensure that any expansion of powers or systems to collect individuals’ information to contain the virus are proportionate and temporary, and that limitations on the potential misuse of information are in place.

Equally, genuine engagement with existing freedom of information regimes provide a fundamental mechanism to independently scrutinise government action, increasing and maintaining trust capital between individuals and their government.

Public authorities must make significant decisions that affect public health, civil liberties and people’s prosperity. As I mentioned earlier, it is imperative that records of these decisions are maintained, including the basis for them, for future generations to scrutinise and learn from. Similarly, preserving the public’s right to access information about such decisions is vital.

Victoria’s Chief Health Officer, Professor Brett Sutton, has thanked Victorians for “overwhelmingly” doing the right thing by staying at home. We have seen tremendous resilience and adaptability in response to COVID-19 within the Victorian community. I believe that this, in part, can be attributed to the trust that Victorians have for our institutions, public service and parliamentary system.

In fact, trust in government in Australia *increased* during the pandemic. The 2021 Edelman Trust Barometer reported a 17-point increase in trust in government, noting an all-time high in trust across Australian institutions.[[2]](#footnote-3)

However, having said that, for the second year in a row Australia recorded the largest trust inequality gap on record globally. This means that Australia has the largest gap in reported trust between the informed public and the mass population. We still have work to do.

If I can sum up my points here, it is that government must do the right thing in line with relevant law as well as community expectations. More than that though, government must *demonstrate* that it is doing the right thing by having openness and transparency wherever possible in the form of regular communication and access to information.

Views on the Privacy Act review

Moving on to my last topic before time for questions: the Privacy Act review.

On 12 December 2019, the Attorney-General announced that the Australian Government would conduct a review of the Commonwealth Privacy Act to ensure privacy settings empower consumers, protect their data and best serve the Australian economy.

The review was announced as part of the government’s response to the Australian Competition and Consumer Commission’s *Digital Platforms* Inquiry.

OVIC provided a submission to this consultation, which is available on the Attorney-General Department’s website for those of you who would like to read our full response.

For the purpose of this presentation, I will briefly touch on three main points from our submission:

* First, the principles‐based approach in the Privacy Act provides a good framework for information governance and privacy best practice, as it offers privacy law the flexibility it needs to stay up to date with technological and other developments.
	+ However, to be effective, principles‐ based regulation must be overseen by an appropriately resourced regulator that is able to publish guidance, and in particular to take enforcement action.
	+ The Office of the Australian Information Commissioner regulates information management in a dynamic and large economy as well as an increasingly data‐reliant government, and it should therefore be better resourced to enable it to carry out its functions and responsibilities in regulating a principles‐based approach to privacy.
* Second, in light of the significant increase in the amount of personal information collected, used and disclosed by political parties and small businesses, and changing community expectations, the exemption for these entities under the Privacy Act should be removed.
	+ This would bring the Privacy Act better in line with community expectations, by ensuring that individuals’ privacy is better protected in circumstances where there is currently little to no privacy protection.
* And third, there are challenges with the current consent model in the Privacy Act, particularly in relation to new technologies such as artificial intelligence and the Internet of Things, and community expectations of when their consent should be sought for the collection, use and disclosure of their personal information, and “consent fatigue” in which they are frequently bombarded by requests for data sharing they may not fully understand.
	+ Requirements to provide notices of collection could also be strengthened.
* Thank you.
1. EU General Data Protection Regulation Guidance, OVIC, <https://ovic.vic.gov.au/privacy/eu-general-data-protection-regulation/>. [↑](#footnote-ref-2)
2. <https://www.edelman.com.au/trust-barometer-2021-australia>. [↑](#footnote-ref-3)