**Title**: *‘Protecting Information Rights in a Digital World: Challenges and Opportunities from the Perspective of the Victorian Information Commissioner’*

**Date**: 24 July 2019

**Time**: 9:30am start

**Location**: Melbourne Law School (room TBA)

**Length**: 20mins (approximately 2,800 words)

Introduction

Thank you to the University of Melbourne for hosting the inaugural Digital Citizens Conference and for having me here today to speak to you. The theme for the Digital Citizens Conference this year, ‘New Technologies: Rights, Responsibilities and Regulation’ is of particular interest to me and I am delighted to have the opportunity to explore with you how this theme intersects with the current landscape for information rights in Victoria.

*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.*

As Victoria’s inaugural Information Commissioner, I have observed an enormous amount of change in the information privacy landscape since the inception of the Office of the Victorian Information Commissioner, or **OVIC,** in September 2017, both locally and internationally.

Reflecting on the sheer volume and pace of changes we have seen or been involved with at OVIC, some key topics come to mind – AI, machine learning, big data, data ethics, information sharing, encryption, biometrics, consent, privacy governance – the list goes on.

Increasingly, our lives are being lived in the digital sphere, with technology aiding almost every interaction we have and every transaction we perform. The way that we experience human rights has undoubtedly been impacted by the ubiquity of technology. In particular, our information rights – the protection of our personal information, and the ability to hold government to account through access to information – stand to be challenged.

The rise of technology has the potential to significantly impact individuals’ information privacy – which traditionally refers to an individual’s ability to decide for themselves when, how and for what purposes their personal information is collected, used or disclosed.

These information privacy rights are protected in Victoria under the *Privacy and Data Protection Act 2014,* overseen by my office. Information privacy is one essential element of the broader right to privacy, enshrined under the Victorian Charter of Human Rights and Responsibilities.

So, as ‘digital citizens’, what do we expect from our governments when it comes to protecting our information rights in a digital world? How has the way we’ve previously understood those rights changed with technology? And how do we ensure that the rights we expect, are protected in the digital sphere?

Today, I would like to explore these pertinent questions in three stages:

1. What is the relationship between the citizen and the state in modern society?
2. What is the impact of technology on information rights?
3. What could, *or should*, the future state look like?

The relationship between the citizen and the state in modern society

So I will now share some observations on the changing relationship between the citizen and the state in today’s connected society.

*First, what do we expect from our governments?*

I’m sure all of us in the room will be familiar with the concept of the ‘social contract’ – the idea 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 rights.

Today, this relationship between citizen and state is often played out in terms of an exchange of data – individuals allowing government to access their personal information, for government to use to improve service delivery, policy design, planning or to drive useful innovation.

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

Citizens also have a reasonable expectation that government monitors the policy landscape and intervenes where reforms, or changing technologies, pose a risk to citizens’ enjoyment of their information rights. Citizens are entrusting us with their data and, in return, expect government to drive change in a sensible and transparent manner, and take swift action where their information rights may be compromised. This is precisely what we aim to achieve at OVIC every day.

In the context of rapid digital reforms, I believe it is more important than ever to take a citizen-centric approach to innovation and reform in the public sector, or in developing policy initiatives to account for significant technological change.

Where individuals’ personal data is used by governments to improve service delivery, it can be all too easy to slip into the mindset that individuals are merely recipients of a service, rather than citizens who are owed fundamental rights and protections.

Taking a citizen-centric approach to digital innovation in the public sector means that new reforms or initiatives need to have a strong ethical foundation, with minimum standards of privacy protections built in at the early design phase. Those driving digital innovation in the public sector need to have a sound understanding of how citizens interact with technology and how the technology will enhance outcomes for citizens.

*So, what role does government play specifically in protecting our information rights?*

Considering that privacy is increasingly viewed as a collective, public good, like clean air and drinking water,[[1]](#footnote-1) government has a vital role to play in protecting against (and responding to) both the individual and communal impacts a contravention of information rights may cause.

On an individual level, a privacy breach, for example, has the potential to cause all sorts of harm, from reputational damage to endangering an individual’s life. OVIC plays a role in receiving and conciliating privacy complaints in Victoria.

However, there are also broader societal consequences for breaches of privacy. Consider the insidious nature of so-called ‘fake news’ on our social media channels, as a result of the incremental misuse of individuals’ personal information to eventually cause widespread misinformation and online ‘echo chambers.’

When certain types of information are shown to some and not all online, based on the discriminatory misuse of certain individuals’ personal information, it limits the possibility for meaningful public debate, freedom of thought and expression. It allows political parties, private entities and foreign states to have an unfair and unreasonable influence on fundamental democratic processes that rely on transparency.

With our lives – and for the young people of today, our formative years – being lived out online, it is now more important than ever to ensure governments take action to protect the right to privacy if we want to continue to live in a free and democratic society.

I see two key elements to governments’ role in protecting information rights: to continue to uphold information rights both on an individual level, and to adapt to rising threats to our information rights on a communal level. Not a small task!

The impact of technology on information rights

*I’d now like to move on to consider the impact of technology on our information rights more specifically.*

In considering the continuing applicability of the right to privacy in today’s interconnected world, I think it is important to remember that the right to privacy is an essential *enabling* right, crucial for the realisation of other fundamental rights.

For example, I would argue that the right to privacy and the right to freedom of thought, conscience, religion and belief, are inextricably linked. Yet, many new and emerging technologies are shifting the privacy landscape, challenging some of the core principles underpinning information privacy law.

For example, the very nature of Artificial Intelligence requires vast amounts of information to train and test algorithms, which in turn strains the validity of the collection limitation principle. This founding principle of privacy law is based on the idea of limiting the collection of personal information to only what is necessary for a particular function or activity.

Further, the purpose specification principle reflected in modern privacy laws, which requires individuals to be made aware of the specific purposes for the collection of their information, is challenged by AI’s ability to extract meaning from data, beyond the original purpose for collection.

In considering the continuing applicability of the right to privacy, last year marked the 70th anniversary of the Universal Declaration of Human Rights. The UN High Commissioner for Human Rights, Michelle Bachelet, noted that our international human rights framework has withstood the reforms of the modern age, providing us “the principles we need to govern artificial intelligence and the digital world.”[[2]](#footnote-2)

On this point, I am very interested to hear the Australian Human Rights Commissioner, Mr Ed Santow’s observations on our current human rights framework, in relation to AI in particular. I think our work to ensure the continuing protection of the right to privacy is very much aligned.

*I’d now like to share some thoughts on the impact of technology on government transparency and rights to access information about government decision making – as my office also administers Victoria’s FOI Scheme.*

Historically, FOI regimes have operated to allow access to documents held by government. FOI acts as a mechanism to ensure transparency in government decision making and accountability to the public.

However, technological advancements such as AI-informed decision-making stand to test current mechanisms for holding government to account, like FOI. For example, the manual nature of FOI decision-making means that, largely, decisions by human decision-makers can be explained. Upon review, the initial decision-making process can be traced, more or less, by application of specific provisions under legislation. More importantly, we can simply ask the original decision maker to explain their decision.

By contrast, the opaque nature of AI-informed decision-making means that it will be extremely difficult for current legal frameworks to provide for transparency for this type of decision making. Transparency of decision-making in the public sector is crucial to ensuring individuals can access government information, services and social resources in a fair and non-discriminatory way.

When it comes to emerging technologies such as AI-informed decision-making in the public sector, I urge all of you to really think on a fundamental level and ask yourselves: what is the problem we are trying to solve? Will this technology really enhance outcomes for the public?

*So, in light of emerging technologies and our interconnected world – has the way individuals think about their privacy changed?*

While I am aware of theories like ‘the privacy paradox’ – the observed disconnect between individuals’ online behaviour and claims that they care about their privacy[[3]](#footnote-3) – our work at OVIC confirms to me that people do indeed care deeply about their privacy.

Of course, individuals (or groups of individuals) will value and experience privacy in different ways. The work of OVIC’s Youth Advisory Group, or **YAG**, has certainly proved this point from the perspective of a younger generation. As digital natives, our YAG members have a rich understanding of the implications of our online presence and we continue to learn from them in shaping our own policy perspectives.

The work of the YAG has shown me that our digital presence does not necessarily need to be at odds with our privacy, if we work to create digital environments that respect, rather than erode, individuals’ privacy.

The future state

*Considering all of this, I’d like to share my observations on what our future state may look like.*

There is no doubt that the public has high expectations of regulators and policy makers to represent their interests and steer reforms in a sensible and privacy enhancing way, in the face of technological change.

In the public sector, I have observed a need to build multi-disciplinary teams to be able to respond quickly to a changing policy environment, considering the social, legal and technical implications of new technologies on information rights.

Combining skillsets will allow us to better understand and appreciate the impact of technology on our information rights – ultimately providing better policy outcomes for us all. For those of you who work in the public sector, I encourage all of you to collaborate and be inquisitive – use your own skillset, seek out knowledge and regularly ask questions!

I have also observed a greater need for collaboration between regulators, not only in the context of enforcement activities, but more broadly, to facilitate greater knowledge transfer across sectors and jurisdictions. Indeed, the Consumer Policy Research Centre (**CPRC**), in its recent report *A Day in the Life of Data,* found that policy responses to the mass collection of consumers’ data in our digital economy will intersect across competition, consumer protection, privacy and human rights.[[4]](#footnote-4)

I’m very glad that we are joined today by the CEO of the CPRC, Lauren Solomon, and am looking forward to hearing her commentary on the session.

To increase collaboration, my office recently led the establishment of the Privacy Authorities Australia Policy Group, to increase and facilitate the sharing of expertise and ideas between privacy authorities in other Australian jurisdictions. We recognised a need for this type of forum, as many of the privacy challenges we are facing today are shared by our colleagues in other jurisdictions, both nationally and internationally.

Through this forum, privacy regulators in Australia have already been able to develop a shared understanding of the privacy challenges posed by technological reforms today.

We also continue to collaborate with international counterparts, through our participation in forums such as the Asia Pacific Privacy Authorities forum, the Global Privacy Enforcement Network and the International Conference of Data Protection and Privacy Commissioners.

A key question we grapple with at OVIC is whether our rising digital presence is inherently incompatible with information rights as we know them. Indeed, the distinction between our online and physical selves is being blurred. However, if we all work toward creating positive, privacy-enhancing and respecting online relationships, and transactions that are citizen-centric,[[5]](#footnote-5) I have confidence that our digital presence need not come at the expense of our information rights.

As lawyers, academics, technologists and policymakers, we need to put or heads together to create digital and online environments that respect individuals’ privacy. After all, the right to privacy – in terms of individuals being able to control who sees their personal information online, when their personal information is shared and to what extent – is essential to the development of one’s identity and sense of self. This will not change, so let’s leave a great legacy for generations to come.

*So, what will OVIC’s future work in the digital sphere look like?*

Following on from the publication of OVIC’s *Artificial intelligence and privacy issues paper* in 2018, which I am proud to say was very well-received, OVIC will publish an e-book on AI next month. The e-book is aimed at improving the Victorian public sector’s understanding of AI technologies and applications that affect privacy, information security and information access. The e-book will explore the technical, legal, and social challenges of AI and privacy, with chapters authored by various experts in the field.

OVIC will continue to host expert guest speakers for our regular public forums, exploring topical privacy issues, with a focus on the impact of technology on the way we experience information rights.

We will continue to engage with Victorian public sector agencies seeking to implement reforms that impact on individuals’ privacy, both proactively and where specifically approached by agencies. We want to continue to be an approachable regulator and a source of reliable advice.

Finally, we will continue to work with our Youth Advisory Group to inform our understanding of the privacy challenges facing young people today.

Concluding remarks

Let me conclude by saying that it has been a pleasure to come here and speak to you today. I’m looking forward to hearing from my fellow speakers today, Ed and Lauren. Thank you again to the University of Melbourne for putting on such a high quality program over the next three days.

My colleague, Privacy and Data Protection Deputy Commissioner Rachel Dixon, will be presenting tomorrow on data and privacy and I encourage all of you to go along for what I know will be a fascinating discussion.

There’s a lot going on, so if you haven’t already, I encourage all of you to subscribe to our Twitter feed: @OVIC\_AU, to keep up to date with OVIC’s future work in privacy, FOI and information security in Victoria.

Thank you.

1. Paul Schwartz, ‘Property, Privacy and Personal Data’ (2004) 117 *Harvard Law Review* 2056,2085. [↑](#footnote-ref-1)
2. United Nations, Office of the High Commissioner for Human Rights, ‘70th Anniversary of the Universal Declaration of Human Rights’ (Statement by UN High Commissioner for Human Rights Michelle Bachelet, 20 December 2018) < <https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23983&LangID=E>>. [↑](#footnote-ref-2)
3. See, Susanne Barth and Menno de Jong, ‘The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review’ (2017) 34 *Telematics and Informatics*, 1038. [↑](#footnote-ref-3)
4. Brigid Richmond (Consumer Policy Research Centre), ‘A Day in the Life of Data: Removing the opacity surrounding data collection, sharing and use environment in Australia’ (2019), 41. [↑](#footnote-ref-4)
5. See, Consumer Policy Research Centre, ‘Consumer data and the digital economy – summary report: Emerging issues in data collection, use and sharing’ (2018), 6. [↑](#footnote-ref-5)