Privacy, participation and purpose: how information rights are essential to a society worth living in

*Sven Bluemmel**

At the time the first *AIAL Forum* was published in 1994, Australia's first privacy legislation was five and a half years old. Our first Freedom of Information Act was just about to enter its teenage years, even though it had first been proposed to Parliament some 20 years earlier. Other relevant developments were similarly finding their feet. These included data analytics and artificial intelligence,[1] even though the latter had been conceived much earlier.

While social media as we know it today was still three years away, with the social network service Six Degrees not launching until 1997, mobile phones had been introduced to Australia some seven years earlier. And the very first smart phone, IBM's Simon Personal Communicator, went on sale in the United States in August 1994, just three months after the first issue of this journal. The first iPhone was still 13 years away.

All of these developments have had an important impact on how we communicate and socialise. They have changed how we inform, develop, shape and communicate opinions. Their effect on how we learn, interact, collaborate, unify and divide has been substantial. The impact on our society has been profound.

The purpose of this article is to outline how information laws have developed in Australia, to identify areas in need of further development and to make the case that information rights are essential to a successful democracy that respects human rights.

Information laws

This article will primarily consider privacy laws and freedom of information (FOI) laws as they apply to government, the public sector and to the delivery of public services. I will refer to these collectively as 'information laws'.

There are, of course, other mechanisms that deal with government accountability. These include parliamentary mechanisms as well as legislation establishing oversight bodies such as Ombudsmen, auditors-general and integrity and anti-corruption commissions. Records management and archival legislation also plays a crucial role in ensuring records are made and kept, which allows those other mechanisms to be effective. However, a consideration of these other mechanisms is outside the scope of this article.

It is tempting to see information rights as one of those first-world luxuries to which we can only aspire because, for most of us, our basic survival needs of food, shelter and the like are met. And this is true. However, a similar argument applies to many rights that we hold dear as being hallmarks of a free and fair modern society — for example, rights to freedom

* Sven Bluemmel is the Victorian Information Commissioner.

1 For an investigation of the concept of Artificial Intelligence, its applications and potential regulatory approaches, see C Bertram, A Givson and A Nugent (eds), *Closer to the Machine — Technical, Social, and Legal Aspects of AI* (Office of the Victorian Information Commissioner, 2019) <https://ovic.vic.gov.au/closer-to-the-machine-ai-publication/>.

of expression and religion, the right to a fair trial, equality before the law and protection from torture or inhuman treatment.

I will look first at privacy laws. Article 12 of the *Universal Declaration of Human Rights* states, 'No one shall be subjected to arbitrary interference with [their] privacy, family, home or correspondence, nor to attacks upon their honour and reputation'. The United Nations General Assembly proclaimed the Universal Declaration in 1948 as a common standard of achievement for all peoples and all nations.

In some Australian states and territories, some information rights are similarly enshrined in human rights legislation. For example, the Victorian *Charter of Human Rights and Responsibilities Act 2006* protects the right to privacy as well as the right to take part in public life. Exercising the latter surely requires understanding of, and therefore access to, information about government.

In 1994, only the Commonwealth had passed information privacy legislation, in the form of the *Privacy Act 1988*. With the exception of Western Australia and South Australia, all Australian jurisdictions now have information privacy laws.[2] Some also have laws that specifically govern the handling of health information.[3] All of these laws require the regulated entities to comply with a number of privacy principles when handling personal information and all can trace their origins to the Organisation for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* introduced in 1980 and updated in 2013..

The OECD guidelines, and thus Australian privacy laws, are based on three pillars: the collection limitation, the purpose specification and the use limitation.

In brief, the collection limitation requires that collection of personal information be limited to only what is necessary; personal information should only be collected by lawful and fair means; and, where appropriate, it should be collected with the knowledge and/or consent of the individual. The purpose specification provides that the purpose of collecting personal information should be specified to the individual at the time of collection. Finally, the use limitation provides that personal information should only be used or disclosed for the purpose only for which it was collected, unless there is consent or legal authority to do otherwise.

The underlying goal of these intertwined principles is to minimise the amount of information any one organisation holds about an individual and to ensure that the way the information is handled is consistent with the expectations of that individual. As I will discuss later, the adequacy of these principles is being tested by technology, particularly by analytics and artificial intelligence.

Turning now to the second category, all Australian jurisdictions have laws that give individuals a legislated right to access government information, subject to certain limitations

2 *Privacy Act 1988* (Cth); *Privacy and Personal Information Protection Act 1998* (NSW)*; Information Privacy Act 2009* (Qld); *Personal Information Protection Act 2004* (Tas); *Privacy and Data Protection Act 2014* (Vic); *Information Privacy Act 2014* (ACT); *Information Act 2002* (NT).

3 *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT).

and exceptions. These are variously known as FOI laws,[4] right to information laws[5] or public access laws.[6] For the purposes of this article, I will refer to them generically as FOI laws.

FOI laws are often considered to be primarily tools of government accountability and transparency. While they certainly perform those functions, there is another reason why they are so important to an effective liberal democracy. Access to information allows citizens to participate meaningfully in the processes of government.

The first Australian state with FOI legislation was Victoria, which passed the *Freedom of Information Act 1982* (Vic) in the same year as its Commonwealth counterpart. By 1994, every Australian jurisdiction other than the Northern Territory had similar legislation. By 2003, national coverage was complete.

The relationship between government and citizens

This article primarily analyses the role of information laws that apply to government or to government service delivery, rather than laws that govern the private sector generally. To do this, it is appropriate to look at some aspects of the relationship between government and citizens.

Government has powers that are not generally available to non-government bodies. It is a fundamental aspect of modern democratic societies that we are prepared to give up some of our freedoms for a form of common benefit. Government has the power to regulate conduct. It makes and enforces laws, raises revenue through non-voluntary mechanisms and can even jail people where the law requires it to do so. While some companies are arguably more powerful than some governments when measured by financial or even social influence, they still rely on the existence and enforcement of rules by government in order to operate.

It has become fashionable for governments to refer to their citizens in various contexts as 'customers'. As I have written in this journal previously, this trend should be resisted.[7] A true customer has the freedom to choose a service or product from a competitive marketplace. A person interacting with government generally does not. This monopoly position of the state is counterbalanced by the state's behaviour being subject to limitations and scrutiny which do not apply to the private sector — for example, obligations of transparency under FOI laws and particular requirements to protect privacy and other human rights.

The relationship between citizens and their government is put under particular strain during times of crisis. This year has, of course, seen the world grapple with the COVID-19 pandemic. Much will be written about the factors that contributed to the success and failure of governments' responses to this crisis. One theory that emerged early in the pandemic was that societies ruled by authoritarian governments would be better placed to respond to the

4 *Freedom of Information Act 1982* (Cth); *Freedom of Information Act 1982* (Vic); *Freedom of Information Act 1991* (SA); *Freedom of Information Act 1992* (WA); *Freedom of Information Act 2016* (ACT); *Freedom of Information Act 2002* (NT).

5 *Right to Information Act 2009* (Qld); *Right to Information Act 2009* (Tas).

6 *Government Information (Public Access) Act 2009* (NSW).

7 S Bluemmel, 'Corporatisation and Electronic Records: On a Collision Course with Administrative Justice?' (2011) 66 *AIAL Forum* 33.

situation than liberal democracies.[8] And one can indeed point to individual cases to support this argument.[9] However, one can also point to examples of liberal democracies whose responses have so far been very effective.[10] Similarly, one can point to authoritarian regimes that have so far fared very poorly.[11]

While a robust analysis of the effectiveness of crisis response in various systems of government is beyond the scope of this article, there is one factor that is highly relevant to the role of information laws. That factor is trust. Successful implementation of the measures that are known to be effective in slowing the spread of COVID-19 requires substantial behavioural change by the population. This comes at considerable financial and social cost to individuals. In the absence of the kind of unchecked state power that exists in some undemocratic societies, the extent to which citizens are willing to engage in the behavioural change that their governments say is necessary will depend, to a significant extent, on citizens' trust in those responses and the governments and institutions behind them. A critical factor necessary in liberal democracies to maintain governments' social licence to impose restrictions on freedom of movement and economic trade during the pandemic has been, in part, the provision of timely information and data to inform citizens.

In the context of information laws, there are two key elements to establishing the necessary trust. First, governments must commit to the responsible and proportionate use of citizens' personal information. Second, governments must be honest and open with citizens about governments' efforts. Both of these elements must be subject to effective and independent oversight. It is here that privacy and freedom of information play a crucial role.

The role of privacy

Privacy is generally considered an essential human right. In several jurisdictions around the world, including in two Australian states and one territory, it is enshrined in human rights legislation.[12] The right to privacy enables individuals freely to develop their personality and identity. It is crucial in developing an ability to participate in political, economic, social and cultural life. It is an enabling right that is important for the realisation of other human rights, such as the right to freedom of expression. Can we truly develop our best sense of self unless we are, in some dimension, left alone to do so? Would important social movements such as universal suffrage or civil rights have succeeded if all their adherents had felt under constant surveillance? Will future generations of young adults find their protest songs if all of the music to which they are exposed is curated for them by algorithms?

Many current privacy laws, including all broad information privacy legislation in Australia, are centred on the concept of personal information. The laws then prescribe how such

8 See, for example, Ilan Alon, Matthew Farrell, Shaomin Li, 'Regime Type and COVID-19 Response' (2020) 9(3) *FIIB Business Review* 152–60 <https://journals.sagepub.com/doi/10.1177/2319714520928884>.

9 Ibid.

10 Carl Benedikt Frey, Chinchih Chen and Giorgio Presidente, 'Democracy, Culture, and Contagion: Political Regimes and Countries' Responsiveness to Covid-19' (2020) 18 *COVID Economics* 222–38 <https://cepr.org/sites/default/files/news/CovidEconomics18.pdf#Paper8>.

11 Ibid.

12 *Human Rights Act 2019* (Qld); *Charter of Human Rights and Responsibilities Act 2006* (Vic); *Human Rights Act 2004 (*ACT).

information may be collected, used and disclosed. This is usually formulated in a number of privacy principles with which organisations must comply. These laws are far better than nothing, but two fundamental limitations are becoming apparent.

The first limitation is that the laws only apply to the collection, use and disclosure of *personal information*. Developments such as artificial intelligence, data analytics and the sheer volume of information being collected and inferred mean that my privacy can be infringed very effectively (potentially destructively) by an organisation that does not even know my name. My newsfeed can feed me stories that cater to my hopes, dreams, biases and hatreds, based on information collected and inferred from many sources. If designed cleverly, it may be able to do so without ever using information that would render me personally identifiable. It can then effectively use or sell these insights to businesses, political parties and others. Again, if done cleverly, it does not need to use my name or other personally identifiable information about me to do so. Instead, it just needs to convince the buyer that it can give reliable access to a cohort of users that are particularly receptive to a particular approach. This can be because that cohort is particularly vulnerable; particularly open to political persuasion; predisposed to believing conspiracy theories; or susceptible to racism, misogyny, or fear or outrage.

This leads to the second limitation. Current privacy laws are conceptually transactional in nature and consent features strongly. Practices are permitted where an individual consents. This treats privacy as a private good and theoretically allows each of us to make our own decisions about what is best. The inherent appeal of this approach to our sense of freedom and agency is obvious.

There are, however, limitations to conceiving privacy as a tradeable consumer good, the price of which is determined by the market. Thinking of privacy as something that can be owned also implies that it can be sold.

Following the Facebook / Cambridge Analytica scandal,[13] more people at least claim to value their privacy. In this climate, privacy becomes an asset to companies — a selling point. The market value of privacy increases, and more companies turn their attention to how they can protect privacy to gain and retain customers. However, letting the market decide the value of our privacy is a very risky move. It also raises the existence of the 'privacy paradox' — where people often say they care about privacy but do not end up putting this into action. One of the challenges of privacy is that it usually appeals to people's future selves, but it is often our current selves who urgently require the new app or service and who end up clicking 'I agree' because there is no other meaningful choice, given what feels most urgent at that moment.

Instead of thinking of privacy as a private good, I argue that we should think of it as a public good. The privacy choices we make as individuals result in collective harm or benefit. If enough of us are careless with our privacy choices, micro-targeting in election campaigns becomes worthwhile. The societal harms from this are substantial. Political discourse becomes more polarised and there is less pressure on political parties to be logically or

13 Julia Carrie Wong, 'The Cambridge Analytica Scandal Changed the World — But it Didn't Change Facebook', *The Guardian* (18 March 2019) <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>.

philosophically consistent or coherent. We all suffer when some of us make poor privacy choices, just as we all suffer when some of us choose to pollute the water supply or when some of us choose to ignore evidence-based infection prevention measures. Personal choice is a good starting point, but it has its limitations.

Data insights and joined-up services

The use of information, including information about individuals, can, of course, have tremendous benefit. A particular area of opportunity that has become much more relevant in recent times is that of data analytics.

CSIRO's data sciences arm Data61 describes data analytics as being about seeing patterns, adding insight and understanding the world in new ways. In other words, analytics transforms raw data into new insights and knowledge. This can be used to develop better policy, improve the planning of infrastructure and help to deliver joined-up services. Effective responses to the current pandemic rely heavily on data and analytics. Even the use of genomic sequencing of the SARS-CoV-2 virus helps to analyse the spread of the virus and to contain outbreaks.[14]

Effective analytics does not have to come at the expense of effective privacy protections. Victoria provides an example of an approach that achieves valuable data insights while protecting privacy. Under the *Victorian Data Sharing Act 2017* (Vic), data may be shared for the purposes of informing policy-making, service planning and design. The Act establishes a Chief Data Officer to coordinate these efforts. Data sharing under the Act is subject to clear safeguards, including the de-identification of data and oversight by the Health Complaints Commissioner and by my office.

Other specific legislation deals with information sharing in particular contexts in Victoria, including for the prevention of family violence,[15] the promotion of the wellbeing and safety of children[16] and for quality and safety purposes in the health context.[17] The *Service Victoria Act 2018* (Vic) provides for safeguards and oversight in relation to the use of personal information in the context of joined-up service delivery.

The above examples show that data insights and joined-up service delivery need not come at the expense of privacy, provided privacy issues are considered early and meaningfully in the design of any initiatives.

While privacy will not usually stand in the way of a well-considered and well-designed initiative to share or analyse data for legitimate public purposes, recent history has demonstrated one significant limitation on how data analytics can be safely performed.

14 In this context it is important to note that the genome being sequenced is that of the virus, not the carrier.
15 *Family Violence Protection (Information Sharing and Risk Management) Regulations 2018* made under the *Family Violence Protection Act 2008* (Vic).
16 *Child Wellbeing and Safety (Information Sharing) Regulations 2018* made under the *Child Wellbeing and Safety Act 2005* (Vic).
17 Part 6B of the *Health Services Act 1988* (Vic).

Until several years ago, it was reasonable to hope that it would be possible to de-identify a complex longitudinal dataset about individuals in such a way that the de-identified dataset could be widely published without breaching anybody's privacy, while still remaining useful for analysis and insight. This now looks less likely. Complex, longitudinal unit-level data about people's behaviours is almost certainly re-identifiable, given sufficient context. This was highlighted by two instances where two such de-identified datasets were found to be re-identifiable. One instance dealt with the release of Australian medical billing records in 2016;[18] the other with the release of public transport usage data in Victoria in 2018.[19]

Both cases demonstrate that complex, longitudinal unit-level datasets, which are, of course, the most useful for generating meaningful insights, may not ever be capable of being reliably de-identified. This does not mean that they cannot be used for analysis. It does, however, mean that relying solely on de-identification is dangerous and unlikely to protect privacy. Instead of releasing such dataset broadly, agencies will need to facilitate the analysis in controlled environments. As noted above, the model under the *Victorian Data Sharing Act 2017* provides one mechanism for doing so while enduring appropriate oversight and control.

Participation and accountability

Citizens in a representative democracy should rightly expect government to be something they can participate in, not something they have done to them. Having access to information is as crucial to citizens' ability to participate meaningfully in society as other important rights, such as the right to freedom of expression or the right to vote.

Freedom of information legislation recognises that government does not exist for its own benefit but only to serve and govern for the public good. It is also a tool for accountability and for minimising, or at least exposing, corruption and misconduct. All of these are important factors in the level of citizens' trust in their government and public institutions.

To be fully effective as a tool for public participation in government, FOI laws must allow for citizens to get access to information easily and quickly. Agency FOI decision-makers must similarly administer the legislation in this spirit.

Some Australian jurisdictions have reformed their FOI legislation to place a greater emphasis on proactive and informal release of information. These include Queensland and New South Wales. In jurisdictions such as Victoria, the legislative focus has remained on providing access to documents following receipt of an FOI request. However, there is nothing preventing agencies from providing access to information outside of a formal request, either proactively or informally in response to a general request. Further, legally binding professional standards issued under the legislation in 2019 require agencies to consider whether a document in their possession can properly be provided to an applicant outside the Act.

18 V Teague, C Culnane and B Rubinstein, 'The Simple Process of Re-Identifying Patients in Public Health Records' *Pursuit* (online, 18 December 2017) <https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records>.

19 Office of the Victorian Information Commissioner, *Disclosure of Myki Travel Information* (OVIC, 2019) <https://ovic.vic.gov.au/wp-content/uploads/2019/08/Report-of-investigation_disclosure-of-myki-travel-information.pdf>.

A 2019 Monash University pilot study commissioned by the Office of the Victorian Information Commissioner surveyed six Victorian agencies subject to the *Freedom of Information Act 1982* (Cth) and found proactive release of information by public sector agencies is important, but it needs to be better supported.[20] Pleasingly, that report also found that the vast majority of the FOI practitioners that participated in the study are sincere, passionate and committed to a well-functioning access to information regime in the state.

Looking at FOI through the lens of public participation in government can have a profound impact on how individual access decisions are reached. A common scenario is where a person requests access to documents that inform a decision on a potential infrastructure project. The argument that disclosure of such a document is against the public interest because deliberations are currently at a sensitive pre-decision stage becomes much weaker when one thinks that meaningful public participation in government is an intended outcome of the legislation. Instead, the fact that deliberations are currently at a sensitive pre-decision stage becomes an argument in favour of disclosure.

There is another quite different area where laws intended to achieve transparency and accountability are being challenged. This is in the area of automated decision-making involving some form of artificial intelligence or machine learning. As these tools become more sophisticated, it becomes more difficult (or even impossible) to explain how a particular decision was reached in a particular instance. As current FOI laws create a legally enforceable right to access documents, they are unlikely to be fully effective in allowing a person to obtain a meaningful insight into how automated decisions have been arrived at. This is further complicated by the fact that private sector developers understandably guard their intellectual property jealously and are unlikely to allow public sector organisations access to algorithms and source code in a way that would allow those organisations to give any meaningful explanation of outcomes to citizens.

When ministers and agencies deal with formal and informal applications for government information, their approach, attitude and decisions will either enhance public trust in government or undermine it. This does not necessarily mean that they must always give full access. FOI legislation quite rightly contains exemptions from disclosure. These exemptions reflect Parliament's view that, in some cases, the public interest will not be in favour of disclosure. However, it is important that ministers and agencies approach their decisions with a view to giving effect to Parliament's intention and dealing with applicants fairly, promptly and respectfully. As I have argued above, doing so will earn trust, and trust is an important aspect in a well-functioning democracy.

What should the future hold?

I hope that the discussion above demonstrates that information laws are coming under intense scrutiny in light of rapid technological and societal developments. The way we develop, grow, learn, interact, argue and participate is changing faster than it has ever changed before.

20 Monash University, *The Culture of Administering Access to Government Information and Freedom of Information in Victoria: Pilot Study May–August 2019* (OVIC, 2019) <https://ovic.vic.gov.au/wp-content/uploads/2019/09/Monash-report-FOI-and-Information-Access-Culture-in-Victoria-pilot-study-2019.pdf>.

Some of our information laws and their associated enforcement mechanisms are coping with the changes, but there are areas of increasing strain.

My hope is that we have a meaningful and broad discussion about the kind of society we wish to live in and want to bequeath to future generations. From this, we will be able to identify the information laws that need to be in place to support that vision. Such a discussion should engage with the following questions:

- Are the definitions and key concepts in our information laws still fit for purpose?
- Should privacy laws be limited to regulating the handling of personal information or should they be broader? As discussed above, developments in technology and big data allow a person's privacy to be substantially infringed by an organisation that does not even know that person's identity.
- Is it feasible for privacy laws to continue to be limited to a conception of privacy as a private, transactional issue? Can we as a society agree that there are certain behaviours and practices that we consider to be such unacceptable infringements of our collective privacy and social fabric that they should be prohibited outright?
- Should access to information laws require more proactive and informal release of information? How do we ensure 'transparency by design' in government policy and decision-making processes?
- How do we regulate automated decision-making that affects the rights and responsibilities of individuals?
- Many information rights rely on some concept of what is and is not in the public interest. The interpretations of this can vary considerably, as noted above in the example of whether disclosure of documents relating to a particular infrastructure project is or is not in the public interest. Is it feasible to develop a common legislated approach to how this is interpreted?

Much work and thought is already being devoted to answering these questions. The ramifications are broad, and all parts of society must have the opportunity to be part of the conversation.

A final thought

I hope that I have made a persuasive case that information rights matter a great deal. They matter not just to the concept of accountability and the prevention of wrongdoing but also to whether we truly live in a free and participatory society where each of us can develop to our best potential.

Like all rights, information rights are not absolute. They coexist with other rights and sometimes that coexistence leads to tensions that need to be addressed. They also exist in the context of rapid technological and social developments, some of which can strengthen our society and some of which can weaken it. But ultimately we need to choose which kind of society we want to live in.

Coming back to the title of this article, are information rights essential to a society worth living in? It depends on whether we want to be able to develop fully as individuals. It depends on whether we want to enjoy personal freedoms. It depends on whether we want to participate in our democracy. And it depends on whether we want those who wield executive power to be accountable to us, the people. If the answer to any of those questions is yes then information rights are indeed essential to a society worth living in.