Office of the Victorian Information Commissioner

# The right to privacy in the digital age

## Submission to the Office of the High Commissioner for Human Rights

The Office of the Victorian Information Commissioner (**OVIC**) was established on 1 September 2017, bringing together the functions of the former Commissioner for Privacy and Data Protection, and former Freedom of Information Commissioner. OVIC is the first regulatory body in Australia to have combined oversight of information privacy, protective data security, and freedom of information.

The privacy law that applies in the state of Victoria, Australia, the *Privacy and Data Protection Act 2014* (**PDP Act**), applies to Victorian public sector organisations including government departments and agencies, universities, municipal councils, and service providers engaged to perform a service on behalf of government.[1] Each of these organisations has obligations in relation to the collection and handling of Victorians' personal information.

OVIC is pleased to make this submission to the Office of the High Commissioner for Human Rights (**OHCHR**) on the right to privacy in the digital age. The comments below are provided in response to the broad themes contained in the OHCHR call for input. They are intended to provide an overview of the recent developments and impact on privacy regulation in the Victorian public sector.

## Developments in legislation concerning the right to privacy in the digital age

### The right to privacy in Victoria

In addition to the PDP Act, the right to privacy is enshrined in s 13 of the Victorian *Charter of Human Rights and Responsibilities Act 2006* (**the Victorian Charter**).[2] The Victorian Charter provides an ongoing protection mechanism for the right to privacy, acting as a filter for any new Bills introduced into Victorian Parliament. All Bills introduced must be accompanied by a statement of compatibility with the Victorian Charter that explains any possible inconsistencies between the proposed law and the Charter, including the right to privacy.

In practice, the right to privacy in Victoria is protected under a web of legislation.[3] The 10 Information Privacy Principles (**IPPs**)[4] under the PDP Act offer the most comprehensive protections for Victorians' personal information. The benefit of the PDP Act being principle-based is that it allows for the IPPs to be interpreted in time with technological change. The IPPs are technology-neutral[5] and non-prescriptive, allowing (and crucially, encouraging) Victorian public sector organisations to apply the principles in an increasingly digital landscape.

[1] The information privacy provisions of the PDP Act apply to those bodies listed in this paragraph; the protective data security provisions have a more limited application and do not extend to universities or municipal councils.
[2] Victoria is only one of two Australian jurisdictions to have a charter of human rights enacted. The Australian Capital Territory has enacted the *Human Rights Act 2004*.
[3] For example, the privacy of health information is protected under the *Health Records Act 2001*, and some organisations will have privacy obligations stemming from the Commonwealth *Privacy Act 1988*.
[4] Listed in Schedule 1 of the PDP Act.
[5] The IPPs are based on the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Information.

### Recent legislative reforms

Recent legislative reforms to promote information sharing have highlighted the importance of continuing to strike the right balance between the right to privacy and other human rights, such as the right to life.[6] Key information sharing reforms have been enacted in Victoria to promote information sharing in response to family violence.[7] Agencies driving these reforms worked closely with OVIC to ensure that the protections afforded under the PDP Act were only limited to the extent necessary for the operation of the scheme. Recognising that the right to privacy is not absolute, this initiative prioritises the right to life and safety of victims of family violence.

Most notably, 2017 saw the passage of the *Victorian Data Sharing Act 2017* (**the Data Sharing Act**) and the introduction of the *Service Victoria Bill 2017* (**the Service Victoria Bill**). The Data Sharing Act reforms the way the Victorian public sector can use and share government information (including individuals' personal information), with an emphasis on using information to inform policy design and service delivery. The Service Victoria Bill aims to considerably change the way Victorians interact with government, creating digital identities for Victorians, and enabling them to transact with government online. OVIC has played a critical role in the development of both initiatives, ensuring that these reforms are delivered in the most privacy enhancing way possible.

Additionally, there is a growing body of case law and recommended practice that may fill a gap in the legislative protections for the right to privacy in Victoria. Recent development in case law on a federal and state level may indicate the courts' willingness to accept serious invasions of privacy as an actionable wrong.[8] Such an approach will allow individuals to seek relief for breaches of their privacy, outside of the PDP Act and human rights framework in Victoria.

### Consent and the GDPR

Recent developments in social media and the design of government and commercial platforms has highlighted a gap between the legal approach to securing consent – via a long and difficult-to-read privacy statement – and genuine informed consent, in which the person consenting to the collection of information has a clear understanding of the uses to which that information may be put. In Europe, the General Data Protection Regulation (**GDPR**) lays out principles for effective consent standards. OVIC strongly supports initiatives such as GDPR, which improve consent processes and should go some way to re-establishing an environment of trust between individuals, governments and businesses.

## Growing reliance on data-driven technology and biometric data

### Data-driven technology

Technology itself is not inherently at odds with privacy. It is the way technology is designed and deployed that determines the extent to which it can erode, or enhance, individuals' privacy. Just like with any other instance of collecting, using and disclosing personal information in a non-technological environment, if the right protections are identified and implemented, there is little to prevent technology from being any less invasive than if information were collected, stored and transmitted by paper.

Granted, technology can pose challenges to traditional privacy constructs such as use limitation and consent, particularly where big data, artificial intelligence (**AI**) and advanced data analytics are concerned. But it can also provide a solution, such as by recording user preferences for how their personal information is used and with whom it can be shared. For example, the Service Victoria platform builds customer preferences into the system; when establishing an account (which is in itself entirely optional – customers

[6] Enshrined in s 9 of the Victorian Charter.
[7] These reforms were the product of key recommendations from Victoria's Royal Commission into Family Violence in 2016. A summary of the recommendations can be accessed here.
[8] See, *Australian Broadcasting Corporation v Lenah Game Meats* [2002] 208 CLR 199 as applied by Hampel J in the Victorian County Court in *Jane Doe v Australian Broadcasting Corporation* [2007] VCC 281, in ruling that an "invasion, or breach of privacy…is an actionable wrong which gives rise to a right to recover damages according to the ordinary principles governing damages in tort" at [157].

may prefer to transact as a guest) users can choose how they wish to receive communications from Service Victoria; whether or not they want to store payment details for future use; and with which government agencies, if any, the customer wishes Service Victoria to share their information.

### Biometric data

Biometric systems have the potential to be both privacy enhancing, and incredibly invasive. The unique characteristics of a fingerprint for example, can set one individual apart from everybody else whose fingerprint is also in the system; where a fingerprint is required for authentication, this makes it extremely difficult to impersonate another person. Conversely, the fact that a fingerprint is unique also strips away any chance at anonymity.

Because of their accuracy and reliability in being able to correctly identify individuals, biometrics are an attractive tool for law enforcement and national security agencies in responding to and preventing serious crime, and for other agencies in verifying an individual's identity. The Victorian Government is set to contribute the facial images of driver licence holders to a national database that will enhance Australia's capability for face matching.[9] In an initiative like this where there may be a demonstrable public interest in people forgoing some privacy, communication with the public, governance and oversight mechanisms, and effective security become increasingly important. Transparency in reporting will assist the public to understand whether or not the trade-off of privacy for security is warranted.

The digital age may require us to reconceptualise how we think about information privacy. This is not to say that privacy is no longer relevant in the digital age, but that perhaps we need to place more emphasis on 'ethical data stewardship', transparency, and good security once information has been collected, than on limiting information being collected in the first place.

## Government surveillance

As new and improved surveillance technologies become cheaper and more accessible, we are seeing an increase in government organisations choosing to initiate surveillance programs. The most prominent examples from a Victorian perspective are closed-circuit television and body worn cameras, used to investigate or prevent crimes, improve public safety, and enhance national security.

While government surveillance activities can create public value, it is important to consider the privacy risks arising from such activities. Some examples include:

- the misuse of information collected from surveillance activities, where information collected for one purpose is later used for a different purpose
- a lack of transparency around an organisation's surveillance practices or activities
- over-collection of information; and
- unreasonably intrusive surveillance activities.

Given the inevitable privacy risks associated with surveillance, governments should always consider the least intrusive methods for capturing and using information via surveillance technologies. In guidance produced by the former Commissioner for Privacy and Data Protection, a list of best practice principles for overt surveillance activities in public places includes the following:

1. Surveillance use must always be necessary, proportionate and for a legitimate purpose related to the activities of the organisation.

[9] See https://www.homeaffairs.gov.au/about/crime/identity-security/face-matching-services.

2. Individuals are entitled to a reasonable expectation of privacy in public places.

3. Surveillance operators must assess the impact of the proposed surveillance before it is undertaken – for example, by completing a Privacy Impact Assessment.

4. Surveillance use must be consistent with applicable laws and standards.

5. Surveillance should be governed by policies, operating procedures and agreements.

6. Surveillance operators should undergo privacy training prior to use.

7. Surveillance operators must take reasonable steps to inform individuals of the use of surveillance devices.

8. The right of individuals to access their personal information should be respected.

9. Reasonable steps should be taken to secure equipment and protect information gathered through surveillance activities.

10. Disclosure of information gathered through surveillance activities should only occur where necessary for the stated purpose, or for a law enforcement purpose.

11. Information gathered through surveillance activities should be deleted once it is no longer required.

12. Effective review and audit mechanisms should be in place to ensure legal requirements and policies are complied with, and that the program is meeting its intended objectives.[10]

## Encryption and anonymity

The issue of encryption and anonymity in Victoria, and Australia more broadly, has gained publicity against the backdrop of the Australian Government announcing in mid 2017 that it would introduce legislation to compel telecommunications services and platforms to provide access to encrypted communications for intelligence or law enforcement purposes. This announcement sparked a fierce national debate about balancing individuals' interests in using encryption to protect the privacy of their communications, and the Government's interest in accessing those communications for security and law enforcement purposes. The proposed bill has not yet been introduced, yet many experts continue to express concern that introducing 'back doors' to encrypted services will weaken the overall strength of the encryption, and generally does not align with the values underpinned in information privacy law.

The Victorian Government's Cyber Security Strategy does not specifically reference the use of encryption. Rather, Victoria's approach to protective data security is non-prescriptive in that it encourages organisations to implement appropriate security protocols for their unique context and risk profile. There are no established principles or standards of encryption in the Victorian government, however OVIC is of the view that best practices require a robust security toolkit, of which strong encryption is an important element. Undermining encryption for some undermines information security for everyone.

## Procedural and institutional safeguards, oversight mechanisms and remedies

### Remedies for breaches of the PDP Act

Where a suspected or actual privacy breach has occurred within the jurisdiction of the PDP Act, an individual has the right to complain to OVIC. Though the Information Commissioner has no power to make

[10] For further information regarding each principle, see the former Commissioner for Privacy and Data Protection's *Guidelines to surveillance and privacy in the Victorian public sector*, April 2017, available here.

a binding ruling or order for compensation, conciliation can take place to try and resolve the complaint. If this is unsuccessful, an individual may seek further remedies with the Victorian Civil and Administrative Tribunal via a referral from the Information Commissioner.

Where an organisation has seriously contravened, or continuously breaches the IPPs, the Information Commissioner may issue a compliance notice, directing the organisation to comply. It is an indictable offence under the PDP Act to fail to comply within the time specified in the notice. Remedies are also available to individuals under the Victorian Charter in conjunction with an administrative claim.

### Security under the PDP Act

Good security practices are integral to protecting individuals' right to privacy. Under the PDP Act, the Information Commissioner is required to develop, implement and oversee a comprehensive protective data security framework.[11] This includes issuing protective data security standards for the confidentiality, integrity and availability of public sector data, which includes personal information. The Standards and Framework create a robust scheme for managing data security risks in Victoria, encouraging a security risk management capability across the public sector and providing mandatory security requirements for the protection of all public sector data throughout the entire information lifecycle. The Standards that have been developed in Victoria are applicable to both digital and paper-based environments.

The Victorian Protective Data Security Framework is mandatory but non-prescriptive, allowing for flexibility when selecting the most appropriate and reasonable security measures and controls for each organisation. The Framework and Standards acknowledge that privacy and security go hand in hand, as privacy cannot be assured without good security. The Framework recognises that taking steps to protect privacy requires more than ICT security measures, necessitating good governance practices, security throughout the information lifecycle, engaging the right personnel and securing physical environments.

### Role of the regulator

As new legislation is drafted in Victoria, the Information Commissioner within their role as the primary privacy regulator will from time to time be consulted on Bills. The value that a privacy regulator can have in this respect is evident in the Service Victoria Bill and Data Sharing Act, both which incorporated a requirement for mandatory data breach reporting to OVIC, on the encouragement of the Information Commissioner.[12] The ability to influence legislation in this way enhances the oversight mechanisms that the regulator has, allowing for a bigger regulatory role, resulting in increased trust and transparency for both individuals and organisations affected by the legislation.

[11] The Victorian Protective Data Security Framework can be accessed here.
[12] See *Victorian Data Sharing Act 2017*, s 24(3), and *Service Victoria Bill 2017*, s 54(3).