Victorian Privacy Network

Privacy Officer Project

Caitlin Galpin

Project Brief – The Rationale

- Support appointed Privacy Officers to:
  - Build a privacy culture
  - Increase their autonomy
  - Increase widespread privacy compliance

- Put Privacy Management Framework into practice

The Input

- 28 privacy officers
- 21 Victorian Public Sector agencies
- 30+ hours of one-on-one calls

The learnings

- Lack of job clarity
- Lack of formal training/induction
- The importance of ‘soft skills’
- More reactive than proactive
- Common challenges

LEARNING #1

Lack of clarity and consistency in definition and understanding of the role

LEARNING #2

The importance of building relationships and effective communication

LEARNING #3

Reported lack of formal training and induction

LEARNING #4

Handling complaints or enquiries from the public is not the main component of the role

LEARNING #5

Activities undertaken are more reactive than proactive

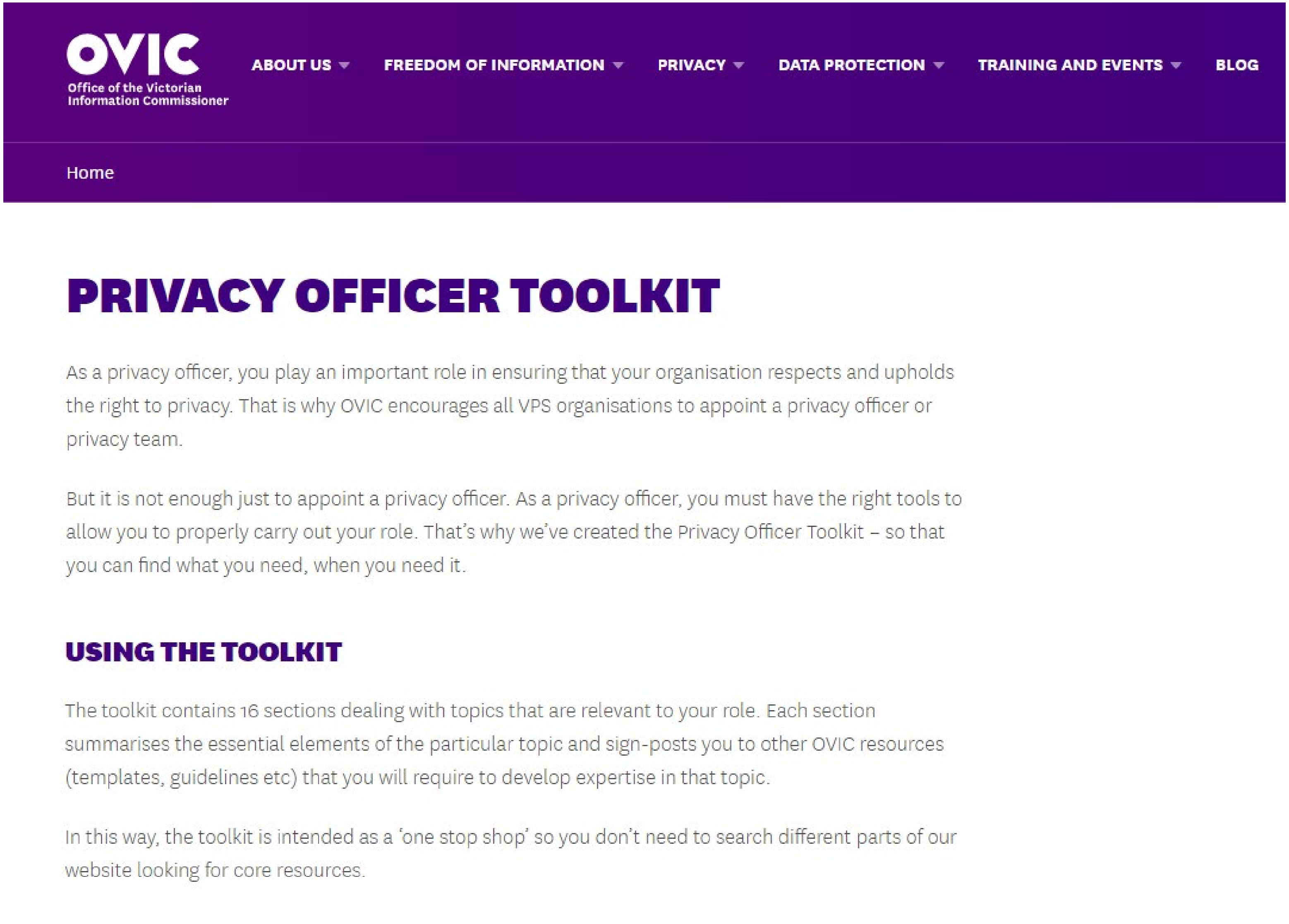
LEARNING #6

The challenge of raising the profile of the role and increasing staff awareness

LEARNING #7

Privacy Officers have trouble finding the tools they need to perform their role

The Toolkit



PRIVACY OFFICER TOOLKIT

As a privacy officer, you play an important role in ensuring that your organisation respects and upholds the right to privacy. That is why OVIC encourages all VPS organisations to appoint a privacy officer or privacy team.

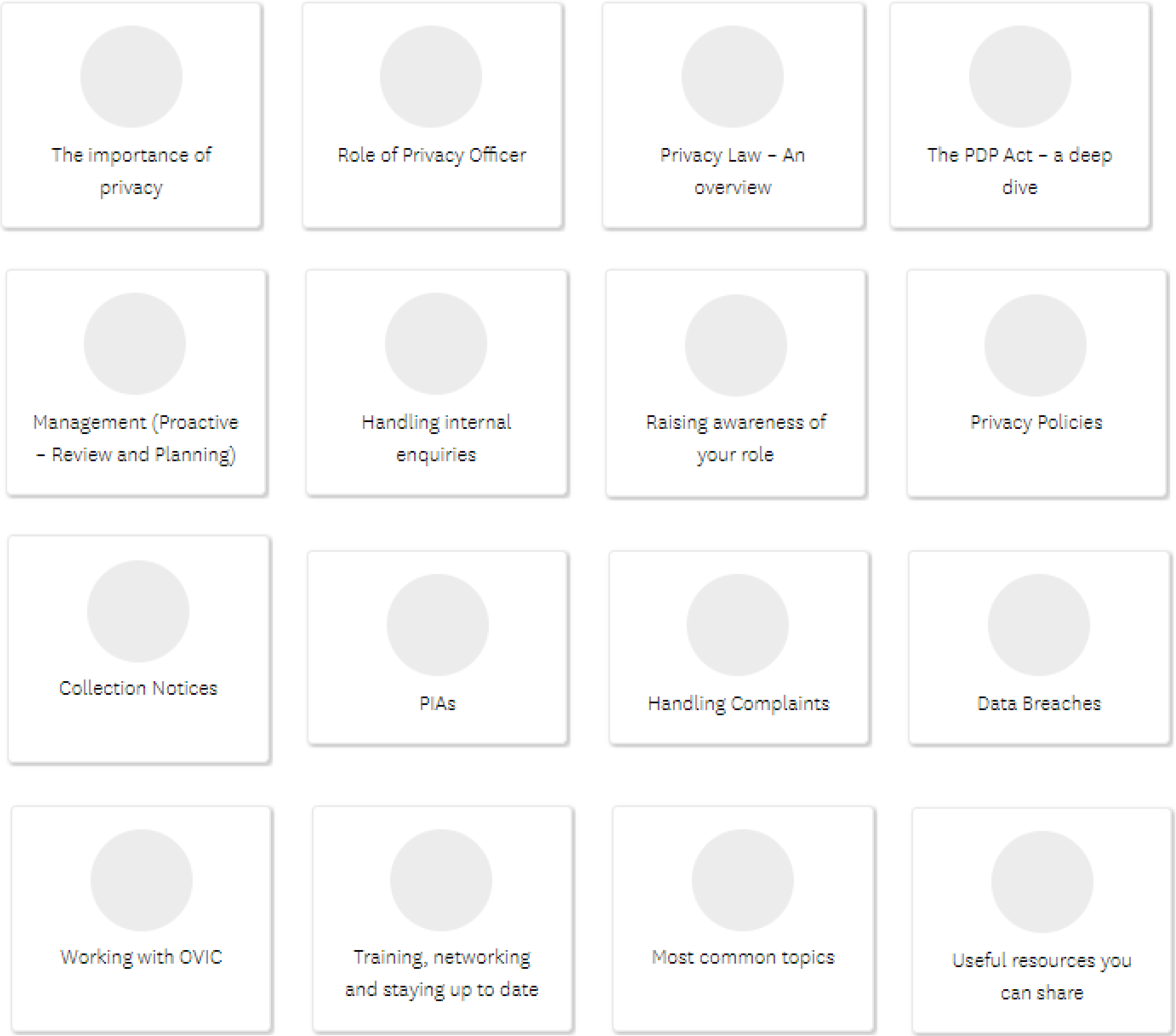
But it is not enough just to appoint a privacy officer. As a privacy officer, you must have the right tools to allow you to properly carry out your role. That's why we've created the Privacy Officer Toolkit – so that you can find what you need, when you need it.

USING THE TOOLKIT

The toolkit contains 16 sections dealing with topics that are relevant to your role. Each section summarises the essential elements of the particular topic and sign-posts you to other OVIC resources (templates, guidelines etc) that you will require to develop expertise in that topic.

In this way, the toolkit is intended as a 'one stop shop' so you don't need to search different parts of our website looking for core resources.

The Toolkit



The importance of privacy

Role of Privacy Officer

Privacy Law – An overview

The PDP Act – a deep dive

Management (Proactive – Review and Planning)

Handling internal enquiries

Raising awareness of your role

Privacy Policies

Collection Notices

PIAs

Handling Complaints

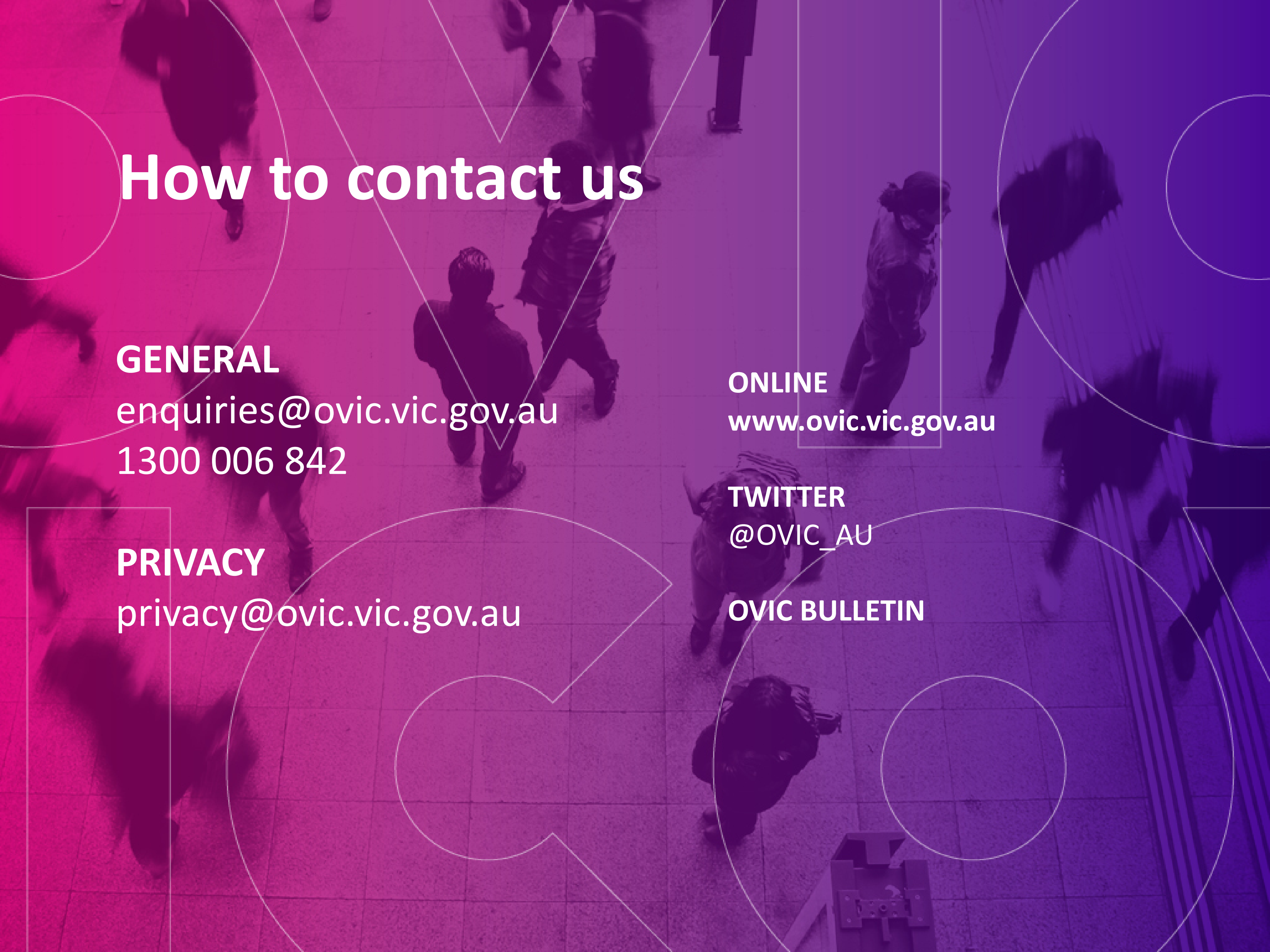
Data Breaches

Working with OVIC

Training, networking and staying up to date

Most common topics

Useful resources you can share



How to contact us

GENERAL
enquiries@ovic.vic.gov.au
1300 006 842

PRIVACY
privacy@ovic.vic.gov.au

ONLINE
www.ovic.vic.gov.au

TWITTER
@OVIC_AU

OVIC BULLETIN

/VICTORIAN**CENTRE**FOR**DATA**INSIGHTS/

Transforming the Victorian Public Service
through data-driven insights

VICTORIA
State
Government

Data Ethics: safeguarding the rights and interests of Victorians as government becomes more data-driven

Presentation to the Victorian Privacy Network

24 March 2021

Victorian Centre for Data Insights

VCDI is the Victorian Government’s centre of excellence for data and analytics. It drives a critical agenda for the public sector.

Our partnerships and projects help deliver key commitments, improve the government’s bottom line, and develop data capability across the VPS.

VCDI also plays a leading role in ensuring that the public sector uses the data that it is entrusted with ethically.

It’s not just big tech and government– we all make ethical choices about data

Technology allows us to lawfully access, collect and use data in ways that were never previously possible.

↓

This fact alone gives rise to ethical judgments we didn’t previously have to make (e.g. when am I crossing a line?).

↓

VCDI encourages its people to start with the principle: just because you can do something with data, it doesn’t mean you should.

Defining and Upholding Data Ethics

- **Data Ethics** describe a code of behaviour, specifically what is right and wrong, encompassing the generation, recording, curation, processing, dissemination, sharing and use of data.*

- Data Ethics should be built on existing ethical norms and values frameworks.

- For instance as the Victorian *Charter of Human Rights and Responsibilities Act 2006* (the Charter) sets out the basic rights and freedoms of all people in Victoria, while a range of other laws protect against discrimination.

- These norms need to be applied to the use of data.

- There is precedent for protecting human rights when using citizen data. Namely, we already have controls in place to protect the *right* to privacy.

- But we need to move *beyond* an exclusive focus on privacy and evolve our controls to keep pace with a growing range of ethical risks.

> "in the context of large-scale data analytics … there is significant risk that government … will lose sight of the fundamental dignity of human beings when datasets flow far beyond the initial point of collection, treating human being as data points rather than individuals."
>
> AHRC – Human Rights and Technology paper

**www.dataversity.net/what-are-data-ethics*

Earning and Keeping Public Trust (Social Licence)

- The term ‘Social Licence’ captures an important concept: knowing where the bounds of acceptability are. Where a project transgresses public expectations, the fact that it was legal can seem a poor defence.
- Views of what is ‘acceptable’ vary. VCDI’s community attitudes research found that those who are most wary about government use of data are often those who most require targeted, data-driven services.
- Accenture’s global study found that the 72% of Australians were open to sharing their personal information with government in exchange for a more personalised customer service experience.*
- Conversely, a 2018 survey conducted by the ANU Centre for Social Research and Methods found that more than 60% of respondents were concerned or very concerned about their data being used by government to make unfair decisions.**
- This can be mitigated by government demonstrating that it takes ethics and fairness seriously in its use of data and AI. To paraphrase a legal saying: *ethics must not only be practised, they must be seen to be practised*

> *“I’m worried about the Government having access to my information for decision making, because I belong to a group that isn’t the majority and isn't always represented by the Government.”*
>
> **Respondent to VCDI survey**

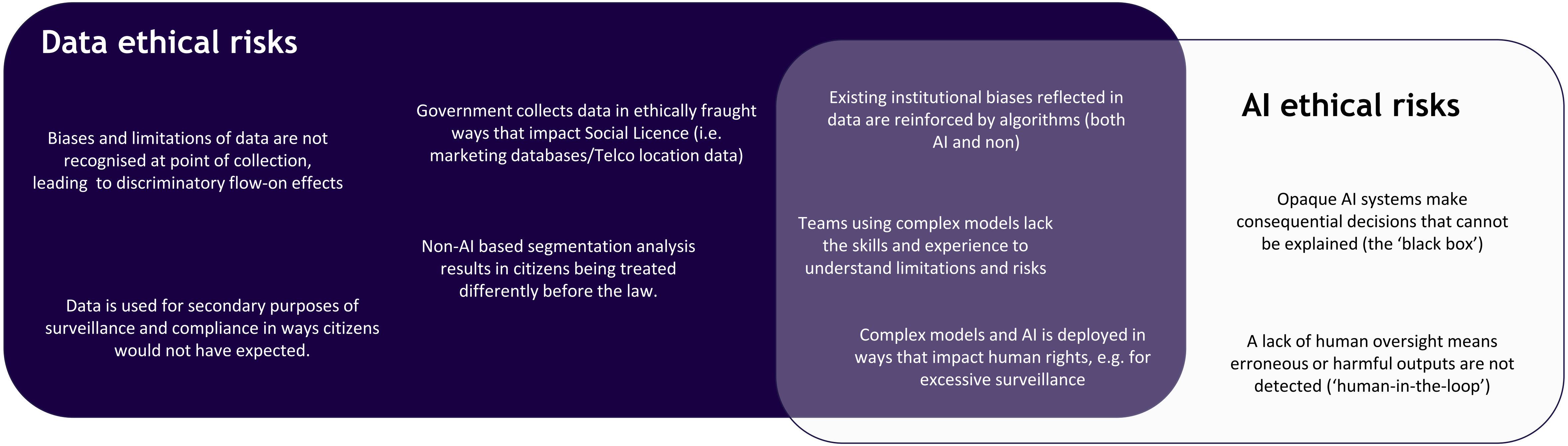
** https://australiancybersecuritymagazine.com.au/citizens-willing-to-share-personal-data-with-government-in-exchange-for-enhanced-customer-services-accenture-survey-finds/*

*** https://theconversation.com/australians-want-to-support-government-use-and-sharing-of-data-but-dont-trust-their-data-will-be-safe-111610*

Data Ethics vs. AI Ethics

The decision whether to frame the conversation around *Data Ethics* or *AI Ethics* is a significant one. Both the Commonwealth and NSW have released policies and principles that focus on AI Ethics. On the other hand, the UK Government set up the Centre for Data Ethics and Innovation and endorsed the *UK Data Ethics Framework*.

VCDI recommends framing the conversation in terms of Data Ethics. Some considerations are quite specific to AI, such as the question of the 'black box' and 'human-in-the-loop'. However, a properly crafted and expansive approach to Data Ethics can capture these considerations.



Data ethical risks

Biases and limitations of data are not recognised at point of collection, leading to discriminatory flow-on effects

Government collects data in ethically fraught ways that impact Social Licence (i.e. marketing databases/Telco location data)

Non-AI based segmentation analysis results in citizens being treated differently before the law.

Data is used for secondary purposes of surveillance and compliance in ways citizens would not have expected.

Existing institutional biases reflected in data are reinforced by algorithms (both AI and non)

Teams using complex models lack the skills and experience to understand limitations and risks

Complex models and AI is deployed in ways that impact human rights, e.g. for excessive surveillance

AI ethical risks

Opaque AI systems make consequential decisions that cannot be explained (the 'black box')

A lack of human oversight means erroneous or harmful outputs are not detected ('human-in-the-loop')

What rights are we trying to protect? (And where does Privacy fit?)

*Victorian Charter of Human Rights**

- Right to privacy and to protect your reputation
- Right to be recognised and treated equally before the law
- Freedom of thought, conscience, religion and belief
- Right to hold an opinion and freedom of expression
- Right not to be arrested or detained unfairly….
- Right to a fair hearing
- Protection of families and children

**This is only a subset of the Charter Rights*

Aboriginal rights

Disability rights

Older people's rights

Racial and religious rights

Employee and workplace rights

LGBTIQ rights

Women's rights

Youth rights

OFFICIAL

Fictional scenario #1

The **Atlantis Department for Child Protection** proposes building an analytics model to inform whether a child is at risk of a family violence incident. This is expected to enable early intervention and prevent several deaths of and serious injuries to children each year.

The project would involve collecting data about families from other agencies, relating to housing, service usage, criminal offending, and recent interactions with case workers. The Department would then build a machine learning model to use patterns in the data to flag where a family demonstrates characteristics that increase the risk to a child.

The project, including the privacy aspects, has been cleared by the Department’s lawyers.

Key considerations

- ❑ Social licence
- ❑ Consultation with affected groups
- ❑ Protection of families and children
- ❑ Algorithmic explainability
- ❑ Human in the loop
- ❑ Capability of teams using sophisticated models

Discussion points

- ○ What are the major ethical risks throughout this project?
- ○ What ethical safeguards could the Department put in place to minimise the risks?
- ○ How could additional safeguards lead to better outcomes for children and families?

Fictional scenario #2

The **Ruritanian Toll Roads Authority** has a significant backlog of unpaid infringements that it is struggling to prioritise and collect.

The Authority wishes to use segmentation analysis to determine the likely reasons that debtors have not paid, based on the number of outstanding infringements and their history of timely payments of tolls and past fines. Debtors will be then grouped into categories, including:

a) Likely to have forgotten
b) Likely to be deliberately evasive
c) Likely to have moved residence
d) Likely to be vulnerable or under financial strain

The Authority will use a new IT system to automatically generate reminder letters and legal demands for categories (a) and (b). Category (c) debtors will be set aside so that the Authority can seek to ascertain their proper address. Mindful of RoboDebt, the debtors in category (d) will be excluded and will not receive automated letters.

Discussion points

- ○ Bearing in mind the safeguards the Department is using, is the approach ethical?
- ○ Are additional safeguards and oversight measures needed?
- ○ Could the project deliver better outcomes for debtors as well as collecting more revenue?

Key considerations

- ☐ Equality before the law
- ☐ Social licence
- ☐ Human in the loop
- ☐ Contestability and administrative review

Fictional scenario #3

The **El Dorado Department of Prisons** has procured a system that uses sophisticated algorithms to determine whether a new prisoner should be kept in a low, medium or high-security facility.

The Department defines the criteria based on previous arrests and convictions, conduct during prior periods of incarceration, documented history of substance abuse, employment history, and history of violence and self-harm. It will not consider race or ethnicity.

The Department is aware that similar decision support tools overseas have led to racially discriminatory outcomes, due to inherent bias in criminal justice data (i.e. certain groups have been more heavily policed and prosecuted).

Key considerations

- ❑ Algorithmic bias
- ❑ Human in the loop
- ❑ Racial discrimination
- ❑ Contestability and administrative review

Discussion points

- ○ How might the project as described lead to discriminatory outcomes?
- ○ What steps could be taken to account for bias and ensure decisions are contestable?
- ○ Could the tool be rolled out in a way that enhances protections for vulnerable prisoners?

Next steps for Victoria?

A comprehensive ethics architecture requires a range of complementary approaches

Legislation and regulation draw clear red lines about what is allowed. This is the most potent tool, and should be used wherever appropriate.

But legislation is slow to develop and change, lacks detail, and cannot codify every ethical issue that may arise. Further, it doesn’t provide practitioners with the *how.* This requires specific policies and ‘soft law’ approaches within government.

Finally, without the skills and capability to recognise and address ethical issues, citizens may not be confident that Data Ethics risks in the Victorian Government are being managed properly.

Legislation & regulatory oversight

There are a range of options to enhance legal protections for Victorians, and to ensure compliance through new or existing regulatory oversight mechanisms.

Policies & ‘soft law’

Codes of practice, frameworks, gateway checks, and effective data governance are critical to embedding ethics in our agencies. The key is to invest in proper design, to ensure these do not become check-box or ‘ethics-washing’* exercises.

Literacy & capability

Literacy and capability at every level is key to upholding data ethics. Leaders need to be aware of risks and accountabilities, and agencies need access to expert guidance and technical skills.

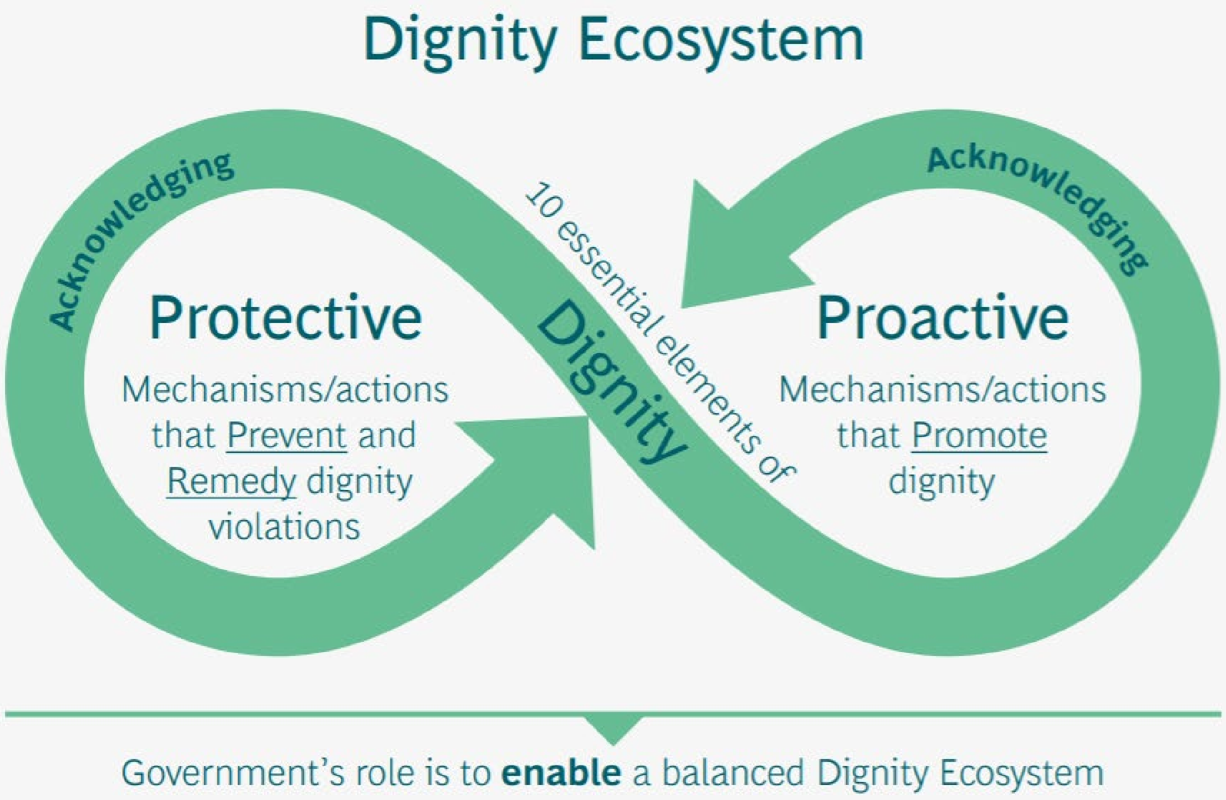
**Ethics-washing’ refers to making a pretence of addressing ethical issues, often to avoid more compliance-based regulation*

A different perspective: the Dignity Lens

New perspective are emerging that government and the private could well benefit from. For instance, a recent report* by Lorenn Ruster from the 3A Institute and Thea Snow from the Centre for Public Impact (A BCG Foundation) advocates that government focus on the role of dignity in its use of AI ethics instruments. This emphasises the proactive role of government in promoting (and not simply protecting) dignity.

Hicks' 10 Essential Elements of Dignity

1. Acceptance of identity
2. Inclusion
3. Safety
4. Acknowledgement
5. Recognition
6. Fairness
7. Benefit of the doubt
8. Understanding
9. Independence
10. Accountability



Dignity Ecosystem

Acknowledging
Protective
Mechanisms/actions that Prevent and Remedy dignity violations
10 essential elements of Dignity
Acknowledging
Proactive
Mechanisms/actions that Promote dignity

Government's role is to **enable** a balanced Dignity Ecosystem

Figure 2: The Dignity Ecosystem

*https://www.centreforpublicimpact.org/assets/documents/CPI-Exploring-the-role-of-dignity-in-government-AI-Ethics-instruments.pdf

Top tips to come out of our consultation with leaders in this space

#	Recommendation
1.	Build out your data ethics approach from existing values frameworks.
2.	Accept that you can’t write rules for every scenario – but where you do see patterns, codify them. (Think OH&S, you don’t have to describe every risk.)
3.	Help your staff develop an ‘ethical switch’ through awareness, training, and repetition. (Again, think OH&S – we’re all drilled to spot hazards in the workplace.)
4.	Make monitoring and enforcement of ethics an extension of your corporate governance. (E.g. build it into risk and data governance practices, including Privacy Impact Assessments.)
5.	Look at ethical challenges through diverse perspectives, ideally by maximising diversity in your data teams and ensuring the voices of data subjects are taken into account.
6.	Acknowledge that good data ethics requires good data, and focus on data management improvements (especially data quality).

Further Reading

Legislation and regulation

Charter of Human Rights and Responsibilities Act 2006 (Vic)
General Data Protection Regulation (EU)
Health Records Act 2001 (Vic)
Privacy and Data Protection Act 2014 (Vic)

Publications

Addressing Trust in Public Sector Data Use, 2020, Centre for Data Ethics and Innovation
AI Ethics Framework, Department of Industry, Science, Energy and Resources
AI Strategy, AI Ethics Policy and AI User Guide, 2020, Government of New South Wales
Artificial Intelligence and Privacy Issues Paper, 2018, Office of the Victorian Information Commissioner
Closer to the Machine: Technical, social and legal aspects of AI, 2019, Office of the Victorian Information Commissioner
Community Attitudes Research, 2017, Victorian Centre for Data Insights (available upon request from VCDI)
Data Ethics Framework, 2018, Government of the United Kingdom
Digital Platform Inquiry: Final Report, 2019, Australian Competition and Consumer Commission
Digital Platform Inquiry Final Report: Submission to the Australian Government, 2019, Office of the Australian Information Commissioner
Digital Platform Inquiry Submission, 2019, Office of the Victorian Information Commissioner
Disclosure of Myki Travel Information, 2019, Office of the Victorian Information Commissioner
Estonia's National AI Strategy, 2019, Government of the Republic of Estonia
Ethical Analytics Toolkit, 2017, Victorian Centre for Data Insights (available on the Innovation Network or upon request from VCDI)
Human Rights and Technology Discussion Paper, 2019, Australian Human Rights Commission
Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry, 2019, Australian Government
Submission in Response to the Artificial Intelligence: Australia's Ethics Framework Discussion Paper, 2019, Office of the Victorian Information Commissioner
Submission in Response to the Artificial Intelligence: Governance and Leadership White Paper, 2019, Office of the Victorian Information Commissioner
Submission in Response to the Human Rights and Technology Issues Paper, 2018, Office of the Victorian Information Commissioner

Webpages

https://australiancybersecuritymagazine.com.au/citizens-willing-to-share-personal-data-with-government-in-exchange-for-enhanced-customer-services-accenture-survey-finds/
https://e-estonia.com/
https://s3.amazonaws.com/external_clips/2956460/7_74342_TrendsinDataGovernanceandStewardship_final.pdf?1547483532
https://theconversation.com/australians-want-to-support-government-use-and-sharing-of-data-but-dont-trust-their-data-will-be-safe-111610
https://www.stats.govt.nz/about-us/data-leadership#legislation
www.dataversity.net/what-are-data-ethics