Office of the Victorian Information Commissioner

t 1300 006 842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D22/17670

21 July 2022

Privacy and Right to Information Reforms
Strategic Policy and Legal Services
Queensland Department of Justice and Attorney-General

By email: PrivacyandRTIreforms@justice.qld.gov.au

Submission in response to Consultation Paper — Proposed changes to Queensland's Information Privacy and Right to Information Framework

Thank you for the opportunity to make a submission in response to the consultation paper on proposed changes to Queensland's information privacy and right to information framework (**Consultation Paper**).

The Office of the Victorian Information Commissioner (**OVIC**) regulates privacy, freedom of information and information security in Victoria. My office administers the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) and the *Freedom of Information Act 1982* (Vic) (**FOI Act**).

As Victoria's Information Commissioner, I have a strong interest in legislative reviews and reforms to information access and privacy laws in other jurisdictions in Australia.

I commend the Queensland Government and Attorney-General for progressing proposed reforms to the *Information Privacy Act 2009* (Qld) (**IP Act**) and *Right to Information Act 2009* (Qld) (**RTI Act**) to ensure they continue to meet changing requirements and community expectations to provide for the protection of personal privacy and timely access to information.

My office considers that most of the proposed changes to the IP Act and RTI Act will improve privacy and access to information in Queensland. In particular, the proposed introduction of a mandatory data breach notification scheme (**mandatory DBN scheme**) is a positive step to improving privacy and information security outcomes in the state.

This submission makes references to the Information Privacy Principles (**IPPs**) contained in Schedule 3 of the IP Act, and to the IPPs contained in Schedule 1 of the PDP Act. When discussing the IPPs in the IP Act, they are referenced as IPPs (Qld). When discussing the IPPs in the PDP Act, they are referenced as IPPs (Vic).

This submission responds to select questions in Part A of the Consultation Paper and provides OVIC's views on proposed changes in Part B of the Consultation Paper.

PART A: PROPOSED PRIVACY REFORMS

Definition of personal information

Response to question 1 — Should the definition of personal information in the IP Act be amended to reflect the definition which is currently in the *Privacy Act 1988* (Cth)?

1. OVIC sees merit in amending the definition of personal information in the IP Act, but cautions against the Consultation Paper's proposal to adopt the current definition in the *Privacy Act 1988* (Cth) (**Privacy Act**).

2. It is uncertain whether the current definition in the Privacy Act captures technical and inferred information.[1] Further, it appears likely the definition in the Privacy Act will be amended in the foreseeable future. The Privacy Act Review Discussion Paper recognises the need for reform,[2] and the Australian Competition and Consumer Commission's Digital Platform Inquiry report and numerous submissions to the Privacy Act Review Discussion Paper support amending the definition.[3]

3. Consequently, if the current definition in the Privacy Act is adopted in Queensland, OVIC is concerned the Consultation Paper will not achieve its objectives of 'consistency with the Privacy Act' and being 'flexible and technology neutral (including to capture a variety of technical data collected in relation to individuals)'.[4]

4. Instead, OVIC suggests the IP Act adopt the proposed amended definition in the Privacy Act Review Discussion Paper:

> Personal information means information or an opinion that relates to an identified individual, or an individual who is reasonably identifiable:
>
> a) whether the information or opinion is true or not; and
>
> b) whether the information or opinion is recorded in a material form or not.
>
> An individual is 'reasonably identifiable' if they are capable of being identified, directly or indirectly.[5]

5. In OVIC's view, adopting the proposed amended definition in the Privacy Act Review Discussion Paper retains a technology neutral definition and ensures a wider range of information, including technical data such as location data, online identifiers, and inferred information, is captured.[6]

6. It would also align the IP Act more closely with global privacy frameworks like the European General Data Protection Regulation (**GDPR**), the California Consumer Privacy Act and Canada's Personal Information Protection and Electronic Documents Act.

---

[1] The uncertainty arises from the decision in *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4. For an explanation see Attorney General's Department, *Privacy Act Review Discussion Paper* (October 2021) (**Privacy Act Review Discussion Paper**), pages 22-25, https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf; Australian Competition and Consumer Commission, *Digital Platforms Inquiry – Final Report* (26 July 2019) (**ACCC DPI report**), pages 459-460, https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.

[2] Privacy Act Review Discussion Paper, page 26.

[3] See ACCC DPI report, pages 459-460, recommendation 16a; Privacy Act Review Discussion Paper, pages 22-24.

[4] Consultation Paper, page 14.

[5] Privacy Act Review Discussion Paper, recommendation 2.1-2.3, page 26.

[6] See OVIC's submission to the Privacy Act Review Discussion Paper (21 December 2021) https://ovic.vic.gov.au/wp-content/uploads/2022/01/Submission-Privacy-Act-Review-Discussion-Paper-December-2021.pdf.

A single set of privacy principles

Response to questions 2 and 3 — Should the proposed Queensland Privacy Principles (QPPs) be adopted in Queensland? If not, in what ways should they be changed?

7. OVIC sees merit in Queensland moving to a single set of privacy principles that align with the Australian Privacy Principles (**APPs**) in so far as possible.

8. The proposed QPP 1, which places a positive obligation on agencies to implement practices, procedures, and systems to ensure compliance with the QPPs, and to ensure agencies can deal with related enquiries and complaints, is likely to have a strongly positive impact.

9. Queensland may wish to further enhance agency privacy governance and accountability by including in QPP 1:

   - a requirement for agencies to *demonstrate* implementation of practices, procedures, and systems. This would support the principle of openness and transparency;

   - a requirement for agencies to implement and demonstrate the steps taken to implement a 'privacy by design' and 'privacy by default' approach. This would direct agencies to actively consider and embed privacy into their information management practices; and

   - the ability for the Office of the Information Commissioner (**OIC**)[7] to request evidence from an agency of the steps taken to ensure compliance with the QPPs, and to implement a 'privacy by design' and 'privacy by default' approach.[8]

10. In relation to the requirement in QPP 1 to 'have a clearly expressed and up to date QPP privacy policy', OVIC suggests that this could be further enhanced by adopting additional language from the GDPR. Specifically, Article 12 of the GDPR requires communications with individuals about information handling practices to be provided 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child'.[9]

11. OVIC otherwise considers the proposed wording of the QPPs to represent a positive change, which could be further improved with a few small amendments. OVIC suggests:

   - Amending QPP 3 to expressly cover circumstances where an agency 'infers, derives, generates or otherwise creates personal information, whether or not that is done by or on behalf of an individual'.[10] This amendment complements the proposal in the Privacy Act Review Discussion Paper to amend the definition of personal information to capture inferred information, and further aligns the protection of personal information with community expectations and international best practice.

[7] For simplicity, this submission uses the abbreviation 'OIC' to refer to functions and powers of the OIC generally, and the exclusive powers of the Queensland Information Commissioner where applicable.
[8] See OAIC's submission to the Privacy Act Review Issues Paper (11 December 2020), recommendation 42, https://www.oaic.gov.au/__data/assets/pdf_file/0018/1773/privacy-act-review-issues-paper-submission.pdf.
[9] See Article 12(a) at https://gdpr-info.eu/art-12-gdpr/.
[10] Proposed in the Privacy Act Review Discussion Paper, page 28, and the OAIC's submission to the Privacy Act Review Issues Paper.

- Amending QPP 5, notice of collection, to include an express requirement that collection notices must be 'clear, current and understandable'.[11] This amendment helps to support an individual's ability to make informed choices, and guards against agencies using lengthy, confusing, outdated, and hard-to-find notices of collection.

- Amending QPP 3 and QPP 6 to include a requirement for collection, use and disclosure of personal information to be 'fair and reasonable'.[12] The inclusion of a requirement for collection, use and disclosure to be both fair and reasonable helps to shift the burden of protecting privacy from the individual to the government, creating a more equitable power balance between agency responsibilities and individual privacy rights. This should also be complemented with OIC guidance or guidelines on the QPPs that calls out the fact that 'unreasonably intrusive collection' or 'disproportionate intrusiveness' will fail the requirement to be fair and reasonable. For example, the requirement would impose an obligation on agencies to assess if their information handling practices are fair and reasonable, even in instances where an individual may have consented to the collection, use or disclosure of their information.

12. OVIC notes that the proposed QPPs do not include an equivalent to IPP 7 (Vic), regulating the assignment, adoption, use, or disclosure of unique identifiers.[13] OVIC suggests an equivalent principle is considered for inclusion in the QPPs. IPP 7 (Vic) is an important privacy enhancing principle that ensures individuals do not become defined by a single number when interacting with government. Regulating unique identifiers also prevents unnecessary and unwarranted data matching across government, and mitigates the impact and harm caused by data breaches by ensuring an individual's 'identity' is not linked to a single number.[14]

13. OVIC suggests enhancing the definition of 'consent' in the IP Act, so it is clear consent means 'voluntary, informed, current, specific, and an unambiguous indication through clear action'.[15] OVIC also suggests that the definition of consent considers an individual's 'capacity' to provide consent. These amendments would go some way to addressing the power imbalance that exists between individuals and government, by encouraging consent to only be sought when an individual is able to exercise a real and meaningful choice about the use or disclosure of their personal information. Concerns over the use of consent as a means of authorising the use or disclosure of personal information are set out in OVIC's submission to the Privacy Act Review Discussion Paper.[16]

14. OVIC generally sees merit in adopting the definition of 'sensitive information' in the Privacy Act. In particular, the specific inclusion of biometric information as sensitive information goes some way to addressing technological advances and community expectations about the treatment of biometric information.

15. OVIC suggests the definition of 'sensitive information' include 'sexual orientation' as well as sexual preferences or practices. This suggested amendment would likely meet community expectations to recognise an individual's sexual identity as sensitive information and, in turn, attribute higher protections to that information.

---

[11] See OAIC's Submission in response to the Privacy Act Review Issues Paper (11 December 2020) page 69 [8.1]. See also OVIC's Submission in response to the Privacy Act Review Discussion Paper (21 December 2021), page 5, https://ovic.vic.gov.au/wp-content/uploads/2022/01/Submission-Privacy-Act-Review-Discussion-Paper-December-2021.pdf.

[12] See Privacy Act Review Discussion Paper, pages 82-85, recommendation 10.1, https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf; OVIC's Submission in response to the Privacy Act Review Discussion Paper (21 December 2021), page 6.

[13] For information about IPP 7 (Vic) — Unique Identifiers, see OVIC's IPP Guidelines https://ovic.vic.gov.au/book/ipp-7-unique-identifiers/.

[14] For example, at the Commonwealth level, disclosure of an individuals' tax file number, does not also mean disclosure of their Medicare number or Centrelink customer reference number.

[15] See Privacy Act Review Discussion Paper, pages 76-78, recommendation 9.1.

[16] OVIC's Submission in response to the Privacy Act Review Discussion Paper (21 December 2021), page 5.

Reasonable steps for the protection of personal information

Response to question 4 — What are the benefits and disadvantages of defining the factors that must be considered in 'reasonable steps' for QPP 9 in the IP Act?

Benefits and disadvantages of defining factors for QPP 9

16. The five common factors listed on page 23 of the Consultation Paper appear to be reasonable principles to guide what it means to 'take reasonable steps' in particular circumstances. In OVIC's view, a regulator should not be more prescriptive than these and should not go down the path of listing controls for agencies to implement. Prescriptive principles could risk controls being missed or overlooked as threats and vulnerabilities evolve. Further, certain controls may not be suitable for some agencies and may not be a suitable use of funds, time, and resources.

17. OVIC notes that the GDPR guidance and the related factors referenced in the Consultation Paper only account for one part of the risk equation. That is, they consider the consequence(s) but not the likelihood of a risk. OVIC suggests a consideration of the 'risk' would be an appropriate additional common factor.

18. OVIC has developed a similar list of factors for organisations to consider when implementing information security, which is a combination of the proposed factors raised in the Consultation Paper and GDPR guidance.[17] OVIC's resource provides guidance on measures to ensure a level of security appropriate to the risk. This includes:

    - Step 1: Identify the organisation's information assets
    - Step 2: Determine the security value of information assets
    - Step 3: Assess any risks to the information assets
    - Step 4: Apply security measures to protect the information assets
    - Step 5: Manage information security risks across the information lifecycle

19. In summary, OVIC takes the approach that you cannot apply security measures (people, process, technical) until you know what information is involved, how sensitive that information is (business impact) and have assessed the risks before looking at applying the relevant controls to manage the risks associated with that information.

Risk of intersection, overlap, and duplication of existing information security policies

20. Based on OVIC's experiences implementing the Victorian Protective Data Security Framework,[18] OVIC notes that care must be taken to ensure any factors that form part of the proposed QPP 9 do not duplicate any existing whole of government information security policies. While privacy and information security go hand in hand, if this occurs, there is a significant risk of causing stakeholder confusion and a duplication of efforts across privacy regulation and information security practices.

[17] See, https://ovic.vic.gov.au/data-protection/the-five-step-action-plan/. Note that the Five Step Action Plan is to assist organisations implement information security practices as opposed to only addressing the security of personal information.
[18] A framework providing direction to the Victorian public sector on their information security obligations. See further information here: https://ovic.vic.gov.au/data-protection/framework-vpdsf/.

21. Evidence from other jurisdictions[19] suggests that security standards issued by government agencies that lack regulatory authority to provide effective assurance mechanisms, have, at best, an irregular record of implementation. There is a place for a regulator with compulsive powers in information security. First and foremost, however, ensuring consistency in advice offered by government agencies requires any regulator to consult extensively with other stakeholders before issuing standards or guidance. Clear and concise communication is key to assisting all stakeholders in navigating this space.

Enhanced powers for the Information Commissioner to respond to privacy breaches

Response to question 7 — Should the Information Commissioner be given a power to conduct an 'own motion' investigation into whether there has been a breach of the privacy principles?

22. OVIC sees merit in the OIC being given the power to conduct own-motion investigations. In OVIC's view there is a strong public interest in equipping an information privacy regulator with the ability to investigate, examine and report on interferences with the privacy of the very individuals the legislation is designed to protect. Investigations, examinations, and public reports offer educatory value to agencies, to help uplift privacy governance and privacy practices, and to inform policy and service delivery decisions for the benefit of the community.[20]

23. In Victoria, the Information Commissioner and the Privacy and Data Protection Deputy Commissioner are empowered to:

- conduct investigations for the purpose of issuing compliance notices under Division 9 of Part 3 of the PDP Act.[21] In practice, this enables OVIC to conduct investigations for the purposes of ascertaining whether the grounds for issuing a compliance notice exist; and

- examine the practice of an organisation with respect to personal information maintained by that organisation for the purpose of ascertaining whether or not the information is maintained according to the IPPs or any applicable code of practice.[22]

24. The PDP Act empowers the Information Commissioner to publish reports and recommendations in the public interest in relation to any act or practice that the Information Commissioner considers to be an interference with the privacy of an individual, or generally relating to the Information Commissioner's functions under the PDP Act. In practice, this enables OVIC to publish investigation and examination reports, where it is in the public interest to do so, and even when the grounds to issue a compliance notice do not exist.[23]

25. Consequently, it appears OVIC's own-motion powers are not limited in the same way as those of the OIC.[24] The OIC may wish to look to the provisions of the PDP Act when considering how to resolve the limitations of the OIC's own-motion investigation, reporting and recommendation powers in the IP Act.

---

[19] For examples on how controls mandated by administrative agencies fail, see the Commonwealth experience (https://www.themandarin.com.au/152046-commonwealth-agencies-failing-to-comply-with-cyber-security-requirements/) and the NSW experience (https://fst.net.au/government-news/auditor-finds-poor-cyber-security-of-significant-concern-for-nsw-agencies-with-all-round-failure-to-adopt-e8-controls/). In Victoria, the Chief Cybersecurity Officer provides advice and capability in responding to issues, and the Victorian Managed Insurance Authority offers advice in risk management in relation to security, but OVIC is responsible for legislated standards and assurance.

[20] For examples, see OVIC's investigation and examination reports on OVIC's website, https://ovic.vic.gov.au/regulatory-action/.

[21] PDP Act, section 8C(2)(e).

[22] PDP Act, section 8C(2)(b).

[23] PDP Act, section 111(3).

[24] Consultation Paper, pages 25-26.

26. When deciding whether or not to take regulatory action to investigate a breach of the IPPs (Vic), it is OVIC's policy to separate out the resolution of an individual privacy complaint from the public interest in undertaking a wider investigation as a result of the complaint. That is, OVIC does not undertake regulatory action for the purposes of enabling action by an individual or individuals following a complaint. In OVIC's view, formal regulatory action involving the use of compulsive powers should be undertaken only when there is a clear public interest in diagnosing and potentially correcting poor practices, to avoid recurrence.

Response to question 8 — Should the Information Commissioner be given a power to make declarations, based on the Commonwealth model, after an own-motion investigation has been conducted?

27. OVIC see merit in the OIC being given a similar power to the Australian Information Commissioner (**AIC**),[25] to make a determination following an own-motion investigation.

28. OVIC suggests the OIC be provided a level of discretion as to when a declaration, investigation report or any associated compliance notices are made public, following an own-motion investigation.

29. In OVIC's experience, there are circumstances where it is necessary to delay the publication of the outcomes of any regulatory action, or delay notifying the public that a compliance notice has been issued. For example, where there may also be criminal prosecutions before the courts, and publication of the notice or publicity around such publication may be potentially prejudicial to such prosecutions. In these circumstances, OVIC's policy is to act promptly where necessary, to issue a compliance notice requiring an agency to remedy defective practices, but to wait until any associated court action is complete before publishing the outcomes of the regulatory action.

Extend the power to make a declaration following a privacy complaint

30. OVIC suggests the proposed declaration power be extended to the making of a determination following *a privacy complaint*. In OVIC's view the power to make a binding determination if conciliation fails, should include the making of declarations similar to:

- the Queensland Civil and Administrative Tribunal's (**QCAT**) powers to declare an act or practice is an interference with privacy and must not be repeated, and to award compensation;[26] and
- the AIC's power to declare that the person or entity must take specified steps within a specified period to ensure that the act or practice is not repeated or continued.[27]

31. OVIC suggests the power to make declarations be coupled with a power for the OIC to publish binding determinations, including reasons. This would ensure transparent outcomes for the community and help inform agencies about how the QPPs should be applied in practice. Decisions by the OIC would still be subject to review at QCAT, thereby ensuring the ongoing determinative role of QCAT.

32. OVIC's suggestion to extend the declaration power to privacy complaints is based on its own experience in administering the PDP Act. OVIC considers that the absence of a power in the PDP Act for OVIC to determine whether the IPPs were breached, award compensation or compel a remedy in circumstances where conciliation has failed can frustrate the achievement of the objects of the Act.

[25] Privacy Act, section 52.
[26] IP Act, section 178.
[27] Privacy Act, section 52.

33. Recognising OVIC's lack of powers, some agencies wait until the matter progresses to the Victorian Civil and Administrative Tribunal (**VCAT**) before fully engaging with the matter or conceding privacy issues. Requiring a complainant to progress to VCAT before receiving a binding determination and relief, including compensation, is also unnecessarily burdensome and time consuming.

34. Allowing the OIC to determine whether there has been a breach of the QPPs, and to award relief including compensation is likely to produce benefits such as:

- allowing the community to obtain an outcome about a privacy breach in a shorter period (weeks or months, rather than years) – quicker outcomes improve access to justice and appropriately recognise privacy as a key community concern;
- effectively deterring agencies from engaging in poor privacy practices, by creating the possibility of quicker remedial action that includes compensation;
- lessening the impact of privacy complaints on agencies by reducing the number of stages they must work through, and legal fees incurred through external representation;
- reducing QCAT litigation where the OIC clearly determines there is no privacy breach, and faster QCAT reviews because QCAT reviews an existing decision; and
- guiding and influencing privacy practices across regulated agencies through a higher frequency of binding determinations by the OIC, that include reasons for the decision, compared with what OVIC assumes is a lower number of QCAT complaints that progress to a binding decision.[28]

35. OVIC recognises that the power to make determinations in privacy complaints would place a resource burden on the OIC. It is a time consuming exercise to gather sufficient information to substantiate findings in a declaration and to draft the corresponding reasons. This has the potential to increase the timeframes for completing complaints and create a backlog of complaints – undermining some of the benefits listed above. Therefore, to achieve benefit from legislative reform, the OIC should also receive appropriate additional funding for any enhanced or new functions.

36. OVIC further suggests that the OIC's power to make a declaration be discretionary. It should not be a mandatory exercise in all privacy complaints. The prioritisation of matters that could be considered to warrant a declaration could be assisted by inserting additional circumstances into the current section 168 of the IP Act that outlines when the OIC may decline to deal with a complaint or to deal with it further. This may include where the OIC is satisfied that the act or practice is not an interference with the privacy of an individual or that the complainant has not suffered any harm as a result of the act or practice specified in the complaint.

Response to question 9 — Should the OIC have the power to intervene in tribunal or court proceedings, involving the IP Act?

37. OVIC sees merit in the proposal for the OIC to be provided with the power to intervene in tribunal or court proceedings involving the IP Act.

38. OVIC see merit in a power for the OIC to apply as a friend of the court, to assist QCAT in matters involving privacy complaints referred to QCAT by the OIC or on review from an OIC decision (in the event the OIC is granted a declaration power to make a binding determination in response to a privacy complaint, as suggested by OVIC in response to question 8 of the Consultation Paper).

[28] In Victoria, only a handful of complaints have made it through the full process and ended with a VCAT decision in favour of the complainant since Victoria first introduced information privacy laws in 2000.

39. OVIC has a similar power to intervene under section 66AB of Schedule 1 of the *Victorian Civil and Administrative Tribunal Act 1998* (Vic). The power to intervene enables OVIC to provide subject matter expertise to VCAT in an impartial manner. Impartial legal submissions in turn assist in levelling imbalances of power between agencies and unrepresented complainants.

40. However, OVIC notes this power has been used sparingly as it is resource intensive, and OVIC's ability to intervene is hampered by lack of visibility as to the arguments being presented throughout the course of a proceeding.

Mandatory data breach notification scheme

Response to questions 11 and 12 — Is the mandatory DBN scheme as outlined in the Consultation Paper suitable for adoption in Queensland? If not, in what ways should it be changed?

41. OVIC considers that adopting a mandatory DBN scheme in Queensland, modelled off the federal Notifiable Data Breaches (**NDB**) scheme, would have considerable merit.

42. OVIC suggests ensuring that state-owned corporations not regulated under the Privacy Act be included in the Queensland DBN scheme, similar to the proposal by New South Wales in its Exposure Draft of the *Privacy and Personal Information Protection Amendment Bill 2021* (NSW) (**NSW Exposure Draft**).[29]

43. OVIC strongly encourages the OIC to publish guidance and resources to assist Queensland agencies assess whether serious harm has or will likely occur. In Victoria, OVIC's guidance and resources are crucial to improving awareness, uptake, and success of OVIC's information security incident notification scheme.[30]

44. OVIC suggests the mandatory DBN scheme require agencies to report a data breach to the OIC even where the risk of serious harm has been mitigated by subsequent actions of the agency.[31] This reporting requirement is included in the NSW Exposure Draft[32] and is best practice in privacy law.[33] This would enable the OIC to assess and evaluate trends across government and within specific agencies, and take proactive educative activities or regulatory action when needed.

45. To be effective, the mandatory DBN scheme needs to be appropriately resourced to allow the OIC to fulfill its proposed expanded functions under the IP Act.[34] The OIC will likely require additional resourcing:

    - to effectively carry out the proposed new investigation and monitoring functions, including conducting reviews, audits, and own-motion investigations; and

    - for communications and guidance, to raise awareness and understanding of the mandatory DBN scheme once introduced.

---

[29] See NSW Government, *Privacy and Personal Information Protection Amendment Bill 2021 Factsheet*, https://www.justice.nsw.gov.au/justicepolicy/Documents/proposed-changes-to-NSW-privacy-laws/privacy-and-personal-information-protection-amendment-bill-2021-factsheet.pdf.

[30] OVIC's incident notification scheme forms an element of the Victorian Protective Data Security Standards issued by OVIC under Part 4 of the PDP Act.

[31] That is, OVIC recommends the Queensland scheme omit the exception for remedial action in section 26WF of the Privacy Act *1988* (Cth).

[32] See NSW Government, *Privacy and Personal Information Protection Amendment Bill 2021* (NSW), Division 3, Subdivision 2, https://www.justice.nsw.gov.au/justicepolicy/Documents/proposed-changes-to-NSW-privacy-laws/privacy-and-personal-information-protection-amendment-bill-2021.pdf.

[33] See Articles 33 and 34 of the *General Data Protection Regulation*.

[34] Consultation Paper, page 32.

46. OVIC suggests including a requirement for Queensland agencies to prepare and publish a data breach policy, similar to section 59ZC of the NSW Exposure Draft.[35] To aid government transparency and improve public trust in government, the data breach policy should include the agencies' processes for reporting suspected eligible data breaches to agency heads.

47. Finally, OVIC suggests the inclusion of an additional exception from the requirement to notify individuals of an eligible data breach. The additional exception would be for situations where notification would create a serious risk of harm to an individual's health or safety, similar to the proposal in the NSW Exposure Draft.[36] OVIC suggests agencies be provided with guidance and examples from the OIC of such situations, to aid decision-making before notifying affected individuals.

OVIC's experiences from introducing an information security incident notification scheme

48. OVIC introduced an information security incident notification scheme as an element in the Victorian Protective Data Security Standards (**VPDSS**).[37] The VPDSS is a legislative instrument issued under sections 86 and 87 of the PDP Act that establishes 12 high level requirements for the Victorian public sector. These are mandatory requirements designed to protect public sector information across all security areas including governance, information, personnel, information communications technology and physical security.

49. Element E9.010 of the VPDSS states 'The organisation notifies OVIC of incidents that have an adverse impact on the confidentiality, integrity, or availability of public sector information with a business impact level (**BIL**) of 2 (limited) or higher'.[38]

50. OVIC's incident notification scheme captures all incidents involving public sector information with a BIL of 2 or higher, whether this includes personal information or not. It should not be confused with a NDB scheme that only captures breaches involving personal information. Nonetheless, OVIC's experiences and learnings introducing its incident notification scheme may be valuable for Queensland to consider.

51. Key lessons OVIC has learnt from the introduction of the incident notification scheme include:

- Keeping the scheme as 'incident notifications' rather than 'breach reporting' allows OVIC to receive information from organisations to conduct analysis without having an active incident response role.

- Notifications of 'incidents' versus 'breaches' allows OVIC to receive information about a security event that compromises the integrity, confidentiality, or availability of a government information asset without organisations needing to ascertain if the event results in a confirmed disclosure or breach.

[35] *Privacy and Personal Information Protection Amendment Bill 2021* (NSW) at https://www.justice.nsw.gov.au/justicepolicy/Documents/proposed-changes-to-NSW-privacy-laws/privacy-and-personal-information-protection-amendment-bill-2021.pdf.
[36] *Privacy and Personal Information Protection Amendment Bill 2021 (NSW),* section 59V, https://www.justice.nsw.gov.au/justicepolicy/Documents/proposed-changes-to-NSW-privacy-laws/privacy-and-personal-information-protection-amendment-bill-2021.pdf.
[37] See https://ovic.vic.gov.au/data-protection/standards/ for further information.
[38] Business Impact Levels are quantitative measures of scaled impacts, that describe the potential impact arising from a compromise of the confidentiality, integrity, and availability of public sector information. For further information see OVIC's Practitioner Guide: Assessing the Security Value of Public Sector Information available here: https://ovic.vic.gov.au/data-protection/practitioner-guide-assessing-the-security-value-of-public-sector-information-v2-0/.

- A Memorandum of Understanding (**MOU**) has been established between OVIC and the Victorian Department of Premier and Cabinet's Cyber Incident Response Service (**CIRS**)[39] to enable the two areas to share incident information. This arrangement has been set up to:

    - Enable information sharing between both offices, to gain greater insight of incidents occurring across the Victorian Government with both offices potentially engaging with different stakeholders within organisations, for example, cyber versus information security versus privacy officers.

    - Reduce the notification and reporting burden on organisations. If organisations engage CIRS to provide incident response capability, they do not need to separately notify OVIC as CIRS will do it on their behalf (a 'no wrong door' approach).

    - Ensure time-sensitive critical incidents can be remediated promptly by CIRS, in recognition that OVIC lacks the 24-hour capability to respond to information security incidents. This is particularly important in the case of ransomware attacks, where the most important priority is restoration of service. Where CIRS responds to critical issues, OVIC allows the notification of the incident from CIRS to substitute for the notification from the affected agency – a 'no wrong door' approach.

- Setting a notification threshold is important. OVIC's threshold requires organisations to notify our office of incidents affecting public sector information with a BIL 2 or higher.[40] This provides OVIC with insights on the incidents that are occurring within the Victorian Government affecting information of greater importance or sensitivity, without being overwhelmed by every single incident occurring.

- Accepting notifications for incidents that involve all information not just personal information, and the compromise of information in any format, for example, cyber, hard copy, and verbal disclosures, provides greater insights and visibility of information handling practices across government.

- Setting a timeframe to receive notifications sets expectations. Understanding OVIC does not provide an incident response service, we provide organisations with up to 30 days to submit a notification, which gives the organisation time to deal with the incident itself and provide timely notification to our office. This timeframe is also consistent with the OAIC's NDB scheme.[41]

- OVIC combined its two separate forms for privacy data breach reporting and information security incident notification to be a single form, so agencies only have to fill in one form. This provides more consistent notifications and reinforces the 'no wrong door' approach.

- Regular insight reports every six-months detailing trends and themes are well received by stakeholders.[42] The six-monthly period also aligns with the OAIC reports so comparisons can be drawn between jurisdictions.

- As awareness of the scheme grows, so too do the number of notifications OVIC receives, which is pleasing to see, but also raises concerns with OVIC's internal resourcing to process the notifications.

[39] Further information about CIRS is available here: https://www.vic.gov.au/victorian-government-cyber-incident-response-service.
[40] See footnote 33 for further information on Business Impact Levels.
[41] See https://www.oaic.gov.au/privacy/data-breaches/.
[42] Incident reports can be viewed at https://ovic.vic.gov.au/data-protection/security-insights/.

- Manual processing of notifications can be labour intensive and a challenge when no additional resourcing is provided. A more automated system to process, analyse and report on incident notifications may be more efficient.

PART B: FURTHER PROPOSED RIGHT TO INFORMATION AND INFORMATION PRIVACY REFORMS

52. This section of OVIC's submission responds to select proposals for changes highlighted in Part B of the Consultation Paper, that aim to clarify and improve the operation of Queensland's information privacy and right to information framework.

Response to proposal for change — A single right of access[43]

Requesting access to documents

53. As the Consultation Paper notes, the current framework for requesting access to government documents in Queensland is split between the RTI Act and the IP Act. The RTI Act provides a right of access to documents of an agency or a Minister, while the IP Act provides a right of access to documents of an agency or a Minister to the extent the documents contain the individual's personal information.

54. The proposed amendments will provide a single right of access under the RTI Act, regardless of whether the requested documents contain an individual's personal information or not. In OVIC's view, this is a positive proposal that would align Queensland's RTI laws more closely with those of other jurisdictions in Australia.

55. The proposal would streamline and simplify the process for individuals, and reduce complications for agencies where requested documents contain a combination of personal and non-personal information. Based on OVIC's experiences, individuals have little difficulty exercising their rights to request information under the FOI Act, regardless of the type of information that is sought.

Amending personal information

56. The Consultation Paper further notes that it is proposed that individuals should apply under the RTI Act, rather than the IP Act, to amend their own personal information. This new right in the RTI Act would replace the existing right under section 44 of the IP Act. It appears a privacy principle in relation to amending personal information would continue to exist in the IP Act, either as IPP 7 (Qld), or the proposed QPP 11.

57. Noting this would reflect the information access framework under the FOI Act and PDP Act, OVIC queries whether it would be beneficial to maintain the right to request an amendment of personal information in the IP Act.[44] In OVIC's view, requests for amendment of personal information naturally and logically fall within legislation regulating personal information, as opposed to legislation providing a right to access information.

58. The public readily understand that rights in relation to their personal information are contained in privacy legislation. Given the right to request access to personal information and the right to request an amendment of personal information are separately outlined in the IP Act, it would be feasible to maintain the amendment provisions as they currently operate in the IP Act.

[43] Consultation Paper, page 36.
[44] OVIC notes that the amendment provisions in section 39 of the FOI Act were in place prior to privacy legislation being enacted in Victoria.

59. OVIC notes that the right to request an amendment under Part V of the FOI Act and a corresponding right under IPP 6 (Vic) have, at times, created uncertainty and confusion as to when and how each right can be exercised by an individual. For example:

- Enquiries OVIC receives from members of the public indicate that individuals are often confused or misunderstand how to request an amendment to their personal information and whether a request should be made under Part V of the FOI Act or IPP 6 (Vic).[45]

- Under section 39 of the FOI Act, it is not beyond doubt whether a document sought to be amended needs to have first been disclosed to an applicant in response to a request for access under the FOI Act, or whether an individual need only have obtained a copy of the document (however so) or be aware of the document's existence and the personal information they wish to have amended. It is OVIC's position that an individual need only have a copy of the document, however obtained, or be aware of the document and information's existence in order to exercise their right to request an amendment under section 39 of the FOI Act.

60. Should the right to request an amendment to personal information be moved to the RTI Act, the purpose of existing IPP 7 (Qld) or proposed QPP 11 must be clear. That is, it should be clearly expressed how the existing IPP 7 (Qld) or proposed QPP 11 differs from the right to request an amendment in the RTI Act, and the circumstances in which either can be exercised by an individual.

61. In OVIC's view, members of the public should be provided a single and clear mechanism to amend personal information in one piece of legislation, as opposed to a right expressed in the RTI Act, and an interrelated or corresponding right expressed as a privacy principle in the IP Act. In OVIC's view this proposal risks creating confusion to those wishing to exercise that right.

62. In addition, OVIC queries whether it would be beneficial for complaint resolution and conciliation under the IP Act (or RTI Act) to include a provision that provides an agency, whether in its discretion or at the request of an applicant, may include a notation to a document that records the applicant's position or opinion, despite an agency refusing to amend a record. For example, the *Mental Health and Wellbeing Bill 2022* (Vic), currently before the Victorian Parliament, contains a mechanism permitting an individual to make a 'health information statement' that must be added to their record by the agency, despite an amendment request being previously denied.[46]

Response to proposal for change — Remove requirement for applications to be in the approved form[47]

63. An individual is currently required use the approved form to make a request under both the RTI Act and IP Act. The Consultation Paper proposes that this requirement be removed.

64. OVIC agrees with the *Review of the Right to Information Act 2009 and Information Privacy Act 2009 Report* that this process is unnecessarily bureaucratic and does not align with any other Australian jurisdiction.[48] In Victoria, no approved form is required, with a request for access to documents or a request for an amendment needing to meet the requirements set out in the FOI Act only.[49] The requirements for making a request under the FOI Act in each circumstance broadly align with the proposed requirements detailed in the Consultation Paper.[50]

---

[45] Section 14(1) of the FOI Act excludes the operation of IPP 6 (Vic) where the amendment relates to a document that can only be requested under the FOI Act. IPP 6 (Vic) is generally applicable to documents held by entities that are subject to Part 3 of the PDP Act, but which are not subject to the FOI Act. In practice, it means that IPP 6 (Vic) is essentially targeted at contracted service providers only.
[46] See the *Mental Health and Wellbeing Bill 2022* (Vic), sections 739-741 at https://content.legislation.vic.gov.au/sites/default/files/bills/591225bi1.pdf.
[47] Consultation Paper, page 37.
[48] See page 51.
[49] FOI Act, sections 17 and 39.
[50] Consultation Paper, page 38.

65. OVIC notes that removing the requirement for an application to be made on an approved form will likely lead to these processes being more accessible for applicants, for example, removing the need to locate and download the form, empowering applicants with poor digital literacy, and assisting those from culturally and linguistically diverse backgrounds.

66. Removal of the approved form will also enable agencies to develop optional context specific forms that may be more relevant and adaptable to the circumstances of the agency and an applicant's requirements. For example, public hospitals in Victoria each have forms that are orientated towards asking questions about the types of medical records applicants most commonly seek and other questions tailored to relevant access processes.

Response to proposal for change — A single period of time for processing applications[51]

67. Amending the RTI Act to provide for a single period of time for processing applications by replacing the concept of a 'further specified period' with an 'extension of the processing period' appears to be a positive reform that would clarify the existing complexities noted in the Consultation Paper.[52]

68. OVIC notes the proposal aligns with the concept of extending the time to make a decision under section 21 of the FOI Act, which enables an agency to extend the period for making a decision:

- by up to 15 days if consultation with a third party is required under certain exemptions; or
- by up to 30 days with the agreement of the applicant.[53]

69. In Victoria, when consultation is required with third parties, an agency is entitled to extend the time for making a decision without the agreement of the applicant. Where an agency seeks an applicant's agreement to extend the time, it may do so any number of times, provided each extension is no more than 30 days and the extension is agreed to prior to the expiry of the existing processing period.[54]

70. In each instance, the agency is required to notify the applicant in writing of the extension.[55]

Response to proposal for change — A new exemption for matters affecting relations with government[56]

71. The Consultation Paper proposes a new exemption that would apply if disclosure of information could reasonably be expected to cause damage to relations between Queensland and another government, or divulge information communicated in confidence by or for another government.

72. It is proposed that this new exemption would be inserted into Schedule 3 of the RTI Act, meaning a decision-maker is not required to apply the public interest balancing test set out in schedule 4 of the RTI Act. Effectively, if the requested information falls within the parameters of this new exemption, then it would be exempt with no regard to the public interest.

73. As noted in the Consultation Paper, Part 4 of Schedule 4 of the RTI Act already contains a public interest version of this proposed new exemption as a factor favouring non-disclosure in the public interest because of public interest harm in disclosure.

[51] Consultation Paper, page 40.
[52] Consultation Paper, page 39.
[53] FOI Act, section 21(2).
[54] FOI Act, section 21(5).
[55] FOI Act, section 21(4).
[56] Consultation Paper, page 43.

74. In OVIC's view, removing the public interest test from intergovernmental communications undermines the principles of open government and transparency, and risks impairing public trust in government decision making. The underlying principles of Australia's administrative law framework are open and accountable government – this includes inter and intra-governmental communications.

75. Information access regimes provide a fundamental mechanism to scrutinise government decisions, including intergovernmental decision-making between Australian jurisdictions. A willingness to be open with the public about intergovernmental decision-making can increase and maintain trust between citizens and the State. This trust is what enables governments to take strong and decisive action and maximise the acceptance and compliance of the public – such as the actions taken during the COVID-19 pandemic.

76. The actions and decisions of government, and the reasons for those decisions and actions, particularly in the context of public emergencies, should continue to be subject to a public interest test, and not based on a subjective 'reasonableness test' as suggested in the Consultation Paper. The exemption, as proposed, risks being used by agencies as a blanket exemption to refuse access to documents in their entirety with no broader consideration of the surrounding circumstances, including, important considerations that weigh the public interest in disclosure versus non-disclosure.

Response to proposal for change — Extend privacy obligations to subcontractors[57]

77. The Consultation Paper proposes an amendment to the IP Act to extend privacy obligations to subcontractors of contracted service providers. The amendment would require contracted service providers to take all reasonable steps to ensure a subcontracted service provider is contractually bound to comply with the privacy principles. In the event of a breach, the privacy complaint would be made against the subcontractor.

78. OVIC agrees with this positive reform, however notes that requiring a contracted service provider and their subcontractors to be contractually bound to the privacy principles should be more than a contractual exercise. In practice an outsourcing organisation should be satisfied that the contracted service provider, and consequentially, any subcontractor, can comply or is compliant with the privacy principles. Merely transferring responsibility or liability does not lead to good or improved privacy practices. It is OVIC's experience that relying on contract provisions without a sufficient assurance program can result in deterioration of processes, and confusion about responsibilities between the parties.[58] Outsourcing to contracted service providers and their subcontractors requires a level of due diligence and assurance on the outsourcing organisation's behalf.

Response to proposal for change — Time limit for applicant to ask Information Commissioner to refer complaint to QCAT[59]

79. The Consultation Paper proposes to amend the IP Act to provide that an applicant has 60 days to ask the Information Commissioner to refer a privacy complaint to QCAT once written notice is provided that the Commissioner does not believe the complaint can be resolved by mediation, or mediation is attempted but is not successful. The existing arrangement does not impose a time limit for the complainant to request a matter be referred to QCAT.

[57] Consultation Paper, page 50.
[58] See OVIC's investigation report into '*Unauthorised access to information held in the CRISSP database, Investigation under section 8(C)2(e) of the Privacy and Data Protection Act 2014*' at https://ovic.vic.gov.au/wp-content/uploads/2021/03/Unauthorised-access-to-client-information-held-in-the-CRISSP-database.pdf.
[59] Consultation Paper, page 53.

80. This is a positive reform that directly aligns with section 71 of the PDP Act, which in OVIC's experience provides a level of certainty to both organisations and complainants as to the outcome of the complaint by ensuring it is not left languishing and open to possible further legal action long after the matter has been raised, and conciliation attempted.

81. This proposal will also enable the OIC to more effectively monitor incoming and outgoing case work and apply appropriate resources to their referral functions and any associated work following the referral.

Consider substituting the terms 'mediation' with 'conciliation'

82. While not discussed in the Consultation Paper, OVIC queries whether in addition to the above proposal for change, a related and subsequent amendment should also be made to section 171 of the IP Act. OVIC suggests that consideration should be given to amending the term 'mediation' to 'conciliation'.

83. In the sphere of alternative dispute resolution, the terms of processes have subtle but different meanings. Mediation is seen as a purely facilitative process where the mediator takes a more hands-off role in terms of the issues, rights, and outcomes in dispute.

84. Conciliation recognises the more active role that a conciliator plays in providing requisite expertise relating to the particular legislative framework. It recognises that the conciliator will play a role in advising the parties to a dispute.

85. Opting for references to 'conciliation' would legitimise an active role by the OIC in advising parties with a view to resolving privacy complaints, such as by offering views on the question of whether there has been an interference with privacy and the appropriateness of options for resolving any interferences.[60]

Response to proposal for change — Amend the definition of 'generally available publication' in the IP Act[61]

86. The Consultation Paper proposes to amend the definition of generally available publication in the IP Act to be consistent with the definition of generally available publication in the Privacy Act, while ensuring that generally available publications which are purely digital (for example, web pages, Twitter feeds, blog posts and Facebook posts) are captured in the definition.

87. While OVIC does not oppose harmonising definitions across jurisdictions, OVIC does query whether all information that is classed as a generally available publication should be exempt from privacy principles.

88. The corresponding exemption for any information contained in a document that is a generally available publication under the PDP Act has the potential to significantly curtail the privacy rights of individuals.[62] This is especially so in the modern context where publications are widely available online and individuals do not always have control over the information that appears about them online.

[60] For more information on the terms, see 'Conciliation: a Discussion Paper' by the Australian Dispute Resolution Advisory Council at https://www.adrac.org.au/_files/ugd/34f2d0_c5795480dc3f4becaf94bb700ed1578a.pdf.
[61] Consultation Paper, page 56.
[62] PDP Act, section 12.

89. Relevantly, the Victorian Supreme Court found that an employee's Facebook posts were not 'a generally available publication' noting that this assessment 'depends upon a consideration of the facts and circumstances as a whole…(t)he nature of the information, the prominence of the Facebook (or Internet website), the likelihood of the access and the steps needed to obtain that access are relevant considerations, among others'.[63] The court's decision highlights that personal information collected from social media sites should not be exempt from privacy protections, on the basis that it is a 'generally available publication'.

90. The exclusion of information contained in generally available publications can lead to undesirable results. For example, under the PDP Act, a person's sexual preferences and practices is regarded as 'sensitive information'. As such, an individual must consent before this information about their sexuality can be collected or used, and various other protections apply to the information under the IPPs (Vic).

91. However, if a generally available publication such as a news article or blog post discloses the individual's sexuality, the information is no longer protected by the PDP Act. Therefore, agencies may freely collect, use, and disclose information about the person's sexuality without regard to the IPPs (Vic) or the PDP Act. This is the case even if the information was published in the news article or blog post against the individual's wishes. In the age of social media and online publication, and advanced analytics tools being utilised by governments, an all-encompassing definition for generally available publications, and exemption from privacy principles undermines privacy protections.

Response to proposal for change — Publication scheme requirements[64]

92. The Consultation Paper proposes that agencies should continue to be required to publish certain information under a publication scheme. However, this information would not be required to be published within an agency's distinct publication scheme or under specific 'classes' of information. As a result agencies would be able to integrate the required information into more relevant parts of their websites, rather than via their publication schemes.

93. OVIC has recently reviewed the obligations for Victorian agencies to publish information and documents as required under Part II of the FOI Act – a similar requirement to publication schemes under the RTI Act. As part of this review, OVIC is preparing to publish new guidance for agencies to follow when implementing the requirements of Part II of the FOI Act.[65] This new guidance significantly departs from the traditional practice of agencies publishing information and documents in standalone 'Part II Statements', a similar practice to the current publication scheme under the RTI Act.

94. Like the Consultation Paper, OVIC recognises that with the rise of technology and agency websites, the way the public interacts with government and searches for information has changed. The public are now able to navigate websites and find information with search engines and website search functions more efficiently.

95. OVIC agrees that agencies should be permitted and empowered to publish relevant information that takes advantage of modern technology such as agency websites and online databases, as well as publishing information and documents in logical and accessible locations and webpages.

Thank you again for the opportunity to make a submission in relation to proposed changes to Queensland's information privacy and right to information laws. I have no objection to this submission being published without further reference to me. I also propose to publish a copy of this submission on the OVIC website.

---

[63] *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285 at [84].
[64] Consultation Paper, page 58.
[65] A consultation draft of this guidance is available at https://ovic.vic.gov.au/wp-content/uploads/2022/05/Draft-Part-II-of-the-FOI-Guidelines-for-public-consultation-Publication-of-certain-documents-and-information-Feedback-due-6-.docx.

If you would like to discuss this submission, please do not hesitate to contact my colleagues Cliff Bertram, Principal Policy Officer or Emma Stephens, Senior Policy Officer, at policyteam@ovic.vic.gov.au.

Yours sincerely

Sven Bluemmel
Information Commissioner