CIPL's Comments on the Australia Attorney-General's Privacy Act Review Report

Response to Government Consultation

Submitted April 6, 2023

I. EXECUTIVE SUMMARY AND RELEVANT CONTEXT FOR CIPL COMMENTS

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond[2] to the Australian Government's consultation[3] seeking comments on the Privacy Act Review Report[4] (PA Review Report) released by the Attorney-General of the Commonwealth of Australia on 16 February 2023. CIPL hopes to inform the Australian Government's response to the Report by emphasising that any modernisation of Australia's privacy laws:

- should be **outcomes-based**, i.e., focusing on intended results rather than specific practices;
- should incorporate principles of **organisational accountability**, which provides flexibility for organisations to tailor compliance measures to their own unique risks and use cases and requires them to be able to **explain** and **validate** their processing decisions when asked by the OAIC;
- should require organisations to perform **contextual risk assessments** and other compliance measures that are demonstrable to the OAIC and other relevant regulators on request; and
- should recognise innovative and flexible legal bases that could be used to support a wide range of data uses;

For more than a decade, CIPL has pioneered organisational accountability as a key building block of effective data privacy regulation and its corresponding implementation within companies. Indeed, **CIPL's Accountability Framework**[5] is a recognised standard for the development of best-in-class data privacy practices and organisational compliance programs.

Figure 1. The CIPL Accountability Framework

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] CIPL is grateful to the Australian Attorney-General's Department for granting us an extension to file comments by 10 April 2023, pursuant to an email dated 27 March 2023.

[3] Government response to the Privacy Act Review Report, available at https://consultations.ag.gov.au/integrity/privacy-act-review-report/.

[4] Privacy Act Review Report 2022, available at https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report.

[5] See CIPL resources and papers on organisational accountability: https://www.informationpolicycentre.com/organizational-accountability.html.

Source: CIPL

Organisational accountability can be used by companies regardless of sector or size. Its **risk-based framework** provides assurance to government regulators and enforcement bodies that companies are identifying and prioritising high-risk data processing. It also simplifies investigations and enforcement actions by requiring companies to be able to demonstrate compliance.

Risk assessments include an evaluation of the "sensitivity" of the data and any risks associated with the intended use of that data, **based on the particular context**, rather than solely on the type of data at issue. Sensitivity and risk-level may vary depending on the context and purpose of use. Thus, instead of attempting to draft definitions on different types of data or categorical classifications such as "sensitive data," **CIPL encourages the publication of guidance** on what might be regarded as "high-risk" data use and processing. This could include guidance on what types of data might be particularly sensitive or high-risk in certain contexts, but the final determination of what, in fact, is sensitive or high-risk should be left to contextual risk assessments. It is the particular **use** of data that creates risks and harms for people, not the data itself.

Risk assessments also help determine whether a particular use in a given context will adversely affect distinct groups of consumers, in specific sectors, or distinct segments of the economy. Risk assessments determine whether certain uses are sensitive and high-risk for certain groups and, therefore, in need of higher protections (e.g., enhanced security measures, limitations on processing purposes or secondary uses, enhanced transparency, effective redress, etc.). Under a risk-based approach, organisations:

(a) build data protection into the design and strategy of their privacy compliance and data governance programs;

(b) assess privacy (and other) risks to individuals and devise appropriate risk mitigations on a continual and context-specific basis; and

(c) document their risk assessments and demonstrate them on request to relevant enforcement authorities, showing that appropriate risk criteria, frameworks, and methodologies are applied.

Any modernisation of Australia's privacy law should thus consider recognising innovative and flexible legal bases that could be used to support a wide range of data uses. Indeed, Australia's privacy regime should provide businesses with **future-proof** legal bases for processing individuals' data.

To encourage and test innovative data uses within a regulated context, CIPL supports **regulatory sandboxes**, **policy prototyping**, and other innovative regulatory methods that address data privacy requirements and compliance challenges associated with new technologies and business practices.

II. SURVEY QUESTIONS

A. PERSONAL INFORMATION, DE-IDENTIFICATION AND SENSITIVE INFORMATION

1. Should there be a criminal offence for re-identifying de-identified information? What exceptions should apply?

> ***Proposal 4.7****: Consult on introducing a criminal offence for malicious re-identification of de-identified information where there is an intention to harm another or obtain an illegitimate benefit, with appropriate exceptions.*

CIPL encourages efforts to incentivise the adoption of good data practices by organisations. When an organisation acts responsibly by de-identifying or anonymising data, a person who intentionally circumvents those efforts for nefarious purposes should be held responsible for such acts.

While CIPL would support legislation that deters re-identification for malicious purposes, a statutory tort could accomplish the same goal, with appropriate exceptions for non-malicious conduct, such as for research involving cryptology, information security and data analysis, and for testing of the effectiveness of security safeguards that have been put in place to protect the information.

Regardless of the particular approach to the prohibition, CIPL also recommends consideration of how to appropriately balance (a) the scope of any re-identification prohibition with (b) the available exemptions and defences. If the scope of the prohibition is wide, then the exemptions and defences need to be extensive and spelled out in detail to ensure that the prohibition does not inadvertently capture appropriate re-identification. It should be made clear that there must be a deliberate and inappropriate attempt to re-identify the data and to use the data in re-identified form.

CIPL also supports further consultation on this issue.

2. Should consent be required for the collection, use, disclosure and storage of other tracking data, such as health data, heart rate and sleeping schedule, in addition to precise geolocation tracking data?

> ***Proposal 4.10:*** *Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent. Define 'geolocation tracking data' as personal information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time.*

CIPL recommends that OAIC issue guidance on tracking practices that would require affirmative opt-in or opt-out consent, but CIPL opposes a blanket consent requirement for all

geolocation tracking, as there are justifiable and legitimate reasons why organisations may collect and use geolocation tracking. For example, ride-hailing companies use geolocation data of drivers and customers to provide and enable the service, to connect drivers with customers, and to ensure safety. Financial institutions may use geolocation data to detect and prevent credit card fraud. Employers may use the geolocation data of their employees to manage a fleet of their vehicles and deliveries. Map services, city transport, and mobility providers all use geolocation data to provide services in a particular context and in a particular moment, and individuals are using these services knowing that their location is important for the provision of the services.

In other words, geolocation data is not always "sensitive," so consent should not be the sole means to permit its use. The very purpose and use of geolocation data would be defeated if individuals could withhold consent. As suggested in the examples above, there are legitimate reasons to collect and use this data in the absence of consent without risk or harm to individuals. In some circumstances location data is necessary for the very provision of the service. In other situations, it may be necessary for the public interest, either health or safety, such as during the Covid-19 pandemic. Instead of requiring consent for all cases involving geolocation data, there should be other legal grounds to process such data as suggested above.

That said, notice to individuals that geolocation tracking is taking place should generally be required, and organisations should conduct robust risk assessments to identify not only potential harms from using geolocation data, but also appropriate measures to mitigate risks. Risk assessments can also help organisations demonstrate why affirmative consent in a specific case would be impracticable, inappropriate, or unnecessary and how the data would be protected against misuse through other means.

Consent is often regarded as a desirable, easy-to-use ground for processing personal data that gives choice to individuals. In practice, however, consent can be cumbersome, transient, and both overwhelming and ultimately meaningless for individuals who face a barrage of requests without the time, inclination, or capacity to review them to the level required for informed decision making. Consent can also be difficult to collect, as it must often meet certain standards to be considered valid. Opt-in consent can induce consent fatigue, which will only increase if more and more digital interactions require consent as data is collected, used, and shared by default in the digital economy. Thus, opt-in consent often undermines and devalues effective privacy protection by discouraging individuals from reviewing privacy notices that purport to provide meaningful notice. Enabling opt-out consent (or implied, or deemed consent) in appropriate contexts can help address some of the problems of opt-in consent (or affirmative express consent).

In light of these constraints, particularly those associated with opt-in consent, CIPL encourages policymakers to consider moving away from viewing the traditional consent model as the sole means to ensure user-centric protection and instead establish an accountability-based model, which places the burden on organisations, not individuals, to prevent harms. This will help deliver far stronger protections for individuals.

Of course, express or opt-in consent should still be enabled where it is appropriate and meaningful, but where it is not appropriate or effective, consumers should be protected through other elements of organisational accountability, such as risk/benefit assessments, risk-based mitigations and safeguards, and rights of redress.

As mentioned in our Executive Summary, risk assessments also include an evaluation of the "sensitivity" of the data and any risks associated with the **intended use** of that data **based on the particular context**. Thus, regardless of whether the data at issue is classified as "tracking data" (whether it be health data, heart rate, sleeping schedule, or precise geolocation data), CIPL believes that a focus on the **data use** (rather than the data type) is more beneficial for all stakeholders.

CIPL would thus reframe the question as not whether a certain data type should require consent, but whether the data at issue **can be used responsibly and with appropriately tailored and proportional protections in a specific context and for a specific purpose.** This approach would be consistent with the "Preventing Harm" principle of the APEC Privacy Framework, which provides that because "risk of harm may result from [ ] **misuse** of personal information, specific obligations should take account of such risk, and remedial measures should be **proportionate to the likelihood and severity of the harm** threatened by the collection, use and transfer of personal information."[6] This approach can only work if the likelihood and severity of harms are considered in connection with specific use cases.

Recent scholarship by Professor Daniel Solove stresses this point in the context of a discussion regarding the classification of certain data types as "sensitive."[7] Professor Solove states that instead of focusing on the **nature** of data—i.e., providing heightened protections for data deemed sensitive (such as precise geolocation information)—laws should focus on **use**, **harm**, and **risk** in specific contexts:

> This Article argues that the problems with the sensitive data approach make it unworkable and counterproductive—as well as expose a deeper flaw at the root of many privacy laws. These laws make a fundamental conceptual mistake—they embrace the idea that the nature of personal data is a sufficiently useful focal point for the law. But nothing meaningful for regulation can be determined solely by looking at the data itself. **Data is what data does. Personal data is harmful when its use causes harm or creates a risk of harm. It is not harmful if it is not used in a way to cause harm or risk of harm**.[8]

By emphasising that it is the **use** of data that matters, not whether it is sensitive or non-sensitive, Professor Solove recognises that there may be appropriate and beneficial uses of data commonly regarded as sensitive: "If privacy laws fail to focus on use, harm, and risk, then they can perversely impede beneficial uses of data."[9]

As illustrated in the examples mentioned above, it is important to remember that not all collection and uses of "tracking data" are bad or harmful. While CIPL agrees that certain uses of data may have an adverse impact in certain contexts, an accountability-based risk assessment will be able to identify such impacts and distinguish low-risk uses from high-risk ones, enable informed decisions as to whether opt-in or opt-out consent should be required,

---

[6] APEC Privacy Framework (2015), Privacy Principle I, (emphasis added), available at https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015).

[7] Solove, Daniel J., *Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data* (January 11, 2023), available at https://ssrn.com/abstract=4322198.

[8] *Id.* p. 4 (emphasis added).

[9] *Id.* p. 46.

and will enable appropriate safeguards for either forms of consent, as well as for "tracking" that might be performed on a basis other than consent.

To aid organisations in conducting robust risk assessments, it would be helpful to issue regulatory guidance and examples on what such high-risk or low-risk data uses might be and to place the burden on organisations to either confirm or negate such high- or low-risk classification in their particular use cases through risk assessments. Finally, this approach keeps consent (opt-in or opt-out) on the table as one particular mitigation option for situations where it would be particularly relevant, meaningful, or appropriate.

B. SMALL BUSINESS EXEMPTION

3. If you are a small business operator, what support from government would be helpful for you to understand and comply with new privacy obligations? (Please select all that apply)

- ☒ Information sessions
- ☒ Written guidance
- ☒ Digital modules
- ☒ Self-assessment tools
- ☒ Financial rebates or tax concessions for obtaining independent privacy advice
- ☒ Other

Generally speaking, it is not the size of the company that matters, but rather the risk and the impact of specific data uses on individuals' rights and privacy. That said, CIPL recognises the need to provide support for small and medium-sized enterprises (SMEs) and start-ups. Consequently, CIPL supports the production of guidance on the use of standard risk assessments for SMEs/start-ups along with other tools. Indeed, the OAIC should make itself accessible for targeted advice to SMEs, especially those that may engage in high-risk processing.

Indeed, large tech companies have recognized that SMEs need help with their compliance obligations and have taken the initiative to provide needed support. For example, Meta's Open Loop Initiative[10] has shown that start-ups clearly benefit from training, tutorials, toolkits, mentorship, and technical assistance to build sound operational governance frameworks and best practices. Open Loop helped start-ups identify and mitigate risks from their AI applications that they may not have addressed otherwise. A similar model could be deployed in Australia, with the help of the OAIC.

As mentioned above, any new privacy obligations should promote an accountability-based framework that requires organisations to collect and use data based on a proper risk assessment. The risk assessment would include an evaluation of the "sensitivity" of the data and any risks associated with the intended use of that data, **based on the particular context**, rather than solely on the type of data at issue.

[10] "Introducing Open Loop, a global program bridging tech and policy innovation," available at https://ai.facebook.com/blog/introducing-open-loop-a-global-program-bridging-tech-and-policy-innovation/.

Sensitivity and risk-level may vary depending on the context and purpose of use. Thus, instead of attempting to draft definitions on different types of data or categorical classifications such as "sensitive data," **CIPL encourages the publication of guidance** on what should be regarded as "high-risk" data use and processing. This could include guidance on what types of data might be particularly sensitive or high-risk in certain contexts. Such guidance could also address relevant risk criteria and consequential harms, and it could **suggest appropriate risk-assessment methodologies** to be used. But the final determination of what, in fact, is sensitive or high-risk should be left to contextual risk assessments. As discussed above, it is the particular use of data that creates risks and harms for people, not the data itself. A similar approach could be taken with low-risk data uses. Guidance could streamline organisational risk assessments by setting forth examples of typically low-risk processing activities, but organisations would be required to ensure that a low-risk classification remains accurate for their particular use cases.

In order to facilitate the standardisation of risk assessments and to avoid unnecessary assessments, it would be useful for the Government to facilitate **engagement and discussions** with stakeholders on appropriate risk taxonomy and methodologies.[11] The regulator should also consider producing **guidance** on the most common high-risk use cases and provide a standard set of mitigating measures that businesses could apply in certain routine situations without the need to conduct a separate or full-blown risk assessment. Of course, such guidance should be directional only; companies would be free to implement different mitigating measures on the basis of a formal risk assessment, in particular if they have reason to believe that in their given context a particular practice might be higher-risk or lower-risk compared to general expectations.

CIPL also supports governmental efforts to help small businesses comply with privacy obligations through the recognition of government-endorsed **certification schemes and codes of conduct**, such as the Global Cross-Border Privacy Rules (CBPR) initiative (which Australia has endorsed). Such formal accountability schemes are particularly invaluable for SMEs because they involve third-party certification bodies (or "Accountability Agents" in the CBPR context) that, in the course of the certification process, help SMEs implement comprehensive privacy and data management programs to comply with the CBPR and/or other applicable requirements. It would be particularly helpful if the OAIC were to articulate more clearly that it will consider participation in such accountability and compliance schemes as a mitigating factor in the enforcement context. That would go a long way towards incentivising and encouraging the uptake of proactive organizational accountability and translate into tangible privacy benefits for consumers.[12]

---

[11] See, for example, CIPL's Draft Risk Matrices contained in CIPL White Paper: *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, June 19, 2014, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf.

[12] *Organizational Accountability in Data Protection Enforcement - How Regulators Consider Accountability in their Enforcement Decisions,* CIPL, October 6, 2021, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organizational_accountability_in_data_protection_enforcement_-_how_regulators_consider_accountability_in_their_enforcement_decisions__6_oct_2021__3_.pdf (filed herewith as Exhibit 3); *CIPL Accountability Discussion Paper 2 - Incentivising Accountability: How Data*

C. EMPLOYEE RECORDS EXEMPTION

4. How should employers provide enhanced transparency to employees about the purposes for which their personal and sensitive information is collected, used and disclosed?

> ***Proposals 7.1:*** *Enhanced privacy protections should be extended to private sector employees, with the aim of:*
>
> *a. providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for*
>
> *b. ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information*
>
> *c. ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and*
>
> *d. notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm.*
>
> *Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact. The possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored.*

The PA Review Report indicates that stakeholders are divided on whether private sector employees' privacy is adequately protected and whether the employee records exemption requires reform.[13] The Report nevertheless concludes that there are legitimate concerns regarding "limited transparency about what employees' personal and sensitive information is being used and disclosed for and whether it is in fact reasonably necessary to administer the employment relationship."[14]

Indeed, processing of employees personal data is becoming a complex compliance topic for many companies operating globally. An increasing number of data privacy and employment laws impose requirements on employers in respect of processing of employees' personal data, but also obligations under employment law. Sometimes, these are in tension—for example, companies need to ensure diversity and non-discrimination in the workplace, based on protected categories of data, yet data privacy laws in some countries restrict how they may be able to collect and use such personal data. Another example is in the realm of information and data security, where employers are expected to put in place measures and systems to

---

Protection Authorities and Law Makers Can Encourage Accountability, CIPL, July 23, 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf.

[13] Privacy Act Review Report 2022, supra note 4, section 7.5.

[14] Id.

protect their data, systems, and networks, including proportionate monitoring of employees' use of such data, systems, and networks. Finally, the Covid-19 pandemic required some employers to monitor remote working, attendance, health, and wellbeing of their employees, all for prudent and legitimate business purposes.

Importantly, over-reliance on consent in the employment context is not always effective, due to the imbalance between the employer and employee. Also, in the examples above, consent would not be the right basis for processing of employee data where this is necessary for performance of employment contracts, compliance with the employer's legal obligation, or other legitimate or public interest. Hence, it is important that the law provides for these additional grounds for processing employees' data and enables companies to use employees' data in the normal course of business activities, from recruitment to employee management, payroll, and other common HR functions. This may also include sensitive personal data where that is necessary for limited purposes, such as compliance with inclusion and diversity obligations and other employment law and non-discrimination laws, or compliance with the provision of health services and insurance, or where data processing is necessary for public interest.

Consultation and engagement with employees is important, and transparency plays an essential role in gaining employees' trust in the system and their understanding of the purposes and value of data processing.

CIPL notes that transparency can serve its purpose only if it is **meaningful**, and in the workplace context, transparency must be meaningful to the employee. Given the increased collection of data from employees in the wake of the Covid-19 pandemic—and given that much of that collection blurred the distinction between work life and personal life—CIPL recognises that employers should provide meaningful transparency regarding new and unprecedented collections of data. Thus, **transparency should be limited to unexpected uses of data, high risk processing, and other non-obvious processing of data**, especially where there may be a fear and a perception of wide and secondary use of such data (even if not true, for negative perceptions are important to address).

Consequently, transparency should be **context-specific, flexible, and dynamic.** It should be adaptable to evolving conditions and changing uses. It must provide clear and understandable information to enable a genuine choice where possible. Meaningful transparency in the workplace is about delivering relevant information to build a trusted relationship between employer and employee. It should explain the benefits of data use, along with organisational accountability and available choices. However, even where choices are not available, transparency is still necessary to provide relevant information about processing activities, risk mitigation measures, individuals' rights, and other accountability-based practices.

CIPL encourages the OAIC to draft guidance on data uses that are particularly high or low risk in the employment context, so that employers, with the help of a contextual risk assessment subject to review by the OAIC, can customize meaningful disclosure based on the unique circumstances of each place of employment.

5. **Noting the current individual rights contained in Australian Privacy Principles 12 and 13, and the proposed individual rights in proposals 18.1, 18.2 and 18.3, what specific exceptions (if any) should apply to these rights in the employment context?**

> ***Proposal 18.1:*** *Provide individuals with a right to access, and an explanation about, their personal information if they request it, with the following features:*
>
> *a. an APP entity must provide access to the personal information they hold about the individual (this reflects the existing right under the Act)*
>
> *b. an APP entity must identify the source of the personal information it has collected indirectly, on request by the individual*
>
> *c. an APP entity must provide an explanation or summary of what it has done with the personal information, on request by the individual*
>
> *d. the entity may consult with the individual about the format for responding to a request, and the format should reflect the underlying purpose of ensuring the individual is informed, as far as is reasonable, about what is being done with their information*
>
> *e. an organisation may charge a 'nominal fee' for providing access and explanation where the organisation has produced a product in response to an individual*
>
> ***Proposal 18.2:*** *Introduce a right to object to the collection, use or disclosure of personal information. An APP entity must provide a written response to an objection with reasons.*
>
> ***Proposal 18.3:*** *Introduce a right to erasure with the following features:*
>
> *a. An individual may seek to exercise the right to erasure for any of their personal information.*
>
> *b. An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.*
>
> *In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement.*

Regarding the exercise of individual rights in the employment context, CIPL notes that the rights to correction and erasure are not absolute rights. They must not compromise an employer's duty to document various aspects of the employment relationship (such as performance assessments) or to use and retain data in order to comply with employment and other legal obligations imposed on the employer.

The right to access should not be overly burdensome or disruptive to business activities and should include exemptions where the right would prejudice the very purpose of data processing—for example, with respect to the use of personal data for the purpose of management decisions or during the performance management process.

While most individuals presumably exercise their rights in good faith, there is a possibility that abuse of these rights—especially for vexatious purposes—may lead to organisations being overwhelmed with requests. Complying with these requests can be disruptive and resource-intensive for organisations and sometimes may involve a disproportionate effort, as when searching for personal data in archived or backed-up files. With clear limitations on the exercise of rights in certain circumstances, organisations can better allocate their resources and prioritise the resolution of legitimate requests. Limitations also help find a balance between data subject rights and other fundamental rights. These limitations should, however, be appropriately balanced so they do not unnecessarily and improperly limit individuals' rights and freedoms, and do not impair individuals' trust in data protection practices.

The Government, therefore, should provide clear boundaries to the exercise of rights in the employment context to address the most impactful uses of employee data and guard against abusive uses that are harmful to employees and disruptive to business activities.

An issue that often arises in the context of access requests is the risk of disclosing third-party personal data. To manage this risk, employers could provide a **structured summary** of the processing activities and a copy of the most relevant data, instead of entire copies of all personal data. If all personal data were in scope, employers would be required to engage in time-consuming and expensive review to remove third-party data, as well as confidential and irrelevant information. Frequently a disproportionate effort is required to collate such information. Thus, CIPL would support a requirement for employers to provide a summary in response to employee access requests that would still provide relevant information in a precise, transparent, and easy-to-understand manner.

As for the right to correction (addressed in Proposal 18.4), it is advisable to clearly define the boundaries of this right to ensure that it only applies to objectively inaccurate data or data that needs to be updated for the purpose(s) for which it is used (for example, because the individual's situation has evolved). An appropriate approach would be to follow the principle pertaining to "Integrity of Personal Information" in the APEC Privacy Framework, which provides that "personal information should be accurate, complete and kept up-to-date **to the extent necessary for the purpose of use**."[15] Similarly, the notion of "accurate/inaccurate" data should apply only to facts and not to opinions. This is also key to protect freedom of expression. Organisations should also be able to ask employees for specific evidence that information held is incorrect.

The right to erasure or deletion enables individuals to request that an organisation erases their personal data, ceases further dissemination of the data, and potentially requires third parties to halt processing of the data. This right is subject to certain caveats, including exemptions for freedom of expression, where the data is required in order to comply with a legal obligation, is needed for fraud prevention purposes, or used in the context of scientific or historical research. Individuals tend to mistakenly believe that erasure is an absolute and unconditional right that applies to all records that an organisation may hold on them. This has led to disputes over ill-framed or controversial requests. As mentioned above, any right to erasure must not compromise an employer's duty to document various aspects of the employment relationship (such as performance assessments) or to use and retain data in order to comply with employment and other legal obligations imposed on the employer.

Lastly, any requirement regarding access to or correction of information should only apply to the entity that has effective control over such information. Processors should not be required to comply directly with rights requests regarding data they process on behalf of an employer, other than to assist the employer in complying with such requests, as appropriate.

[15] APEC Privacy Framework (2015), Privacy Principle VI, (emphasis added), available at https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015).

6. **If privacy protections for employees were introduced into workplace relations laws, what role should the privacy regulator have in relation to privacy complaints, enforcement of privacy obligations and development of privacy codes in the employment context?**

> ***Proposal 7.1:*** *Enhanced privacy protections should be extended to private sector employees, with the aim of:*
>
> *a. providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for*
>
> *b. ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information*
>
> *c. ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and*
>
> *d. notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm.*
>
> *Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact. The possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored.*

To ensure consistency of interpretation, supervision, complaint-handling, and enforcement, CIPL believes that the OAIC should take the primary role with regard to all processing of personal data under Australia's Privacy Act, including the processing of personal data in the employment context if the current exemption were to be modified or removed. As privacy issues are increasingly intertwined with other areas of law—such as online safety, artificial intelligence, children's protection, competition, and employment—it is important that the ultimate regulatory responsibility and oversight is provided by the OAIC and that the OAIC works effectively and collaboratively with their regulatory counterparts in other fields. The establishment of the **Australian Digital Platform Regulators Forum** is an important step towards a more formalised collaboration that will result in more coherent guidance, advice, and action by different regulators.

More broadly, with regard to the enforcement of privacy obligations in the workplace context, the OAIC should promote the adoption of co-regulatory tools—such as codes of conduct or certifications for employee data processing—in consultation with associations representing both employees and employers and other relevant stakeholders. A co-regulatory approach may relieve some of the OAIC's increased regulatory and oversight obligations.

Certification schemes (such as the APEC Cross-Border Privacy Rules (CBPR), soon to become the Global CBPR through the Global CBPR Forum, of which Australia is a member) and codes of conduct involve the use of third-party certifiers or monitoring bodies, as well as dispute resolution providers that are associated with such schemes. These entities can play important front-line enforcement and oversight roles and remediate many issues before the regulator needs to step in. These entities review organisations' compliance and accountability programs and ensure that they comply with the relevant standard to which they were certified. When necessary, they can suspend certifications and take other remedial actions against non-compliant organisations. The dispute resolution functions of these schemes relieve the OAIC

from the burden of dealing with large numbers of "easy" cases, allowing them to focus their enforcement attention on more important and strategic matters.

The benefits of such schemes to regulators are numerous:

- **Reduce oversight workload**: Where certification bodies take on and share with the OAIC the frontline burdens of supervision and oversight with respect to certified entities, this has the potential of reducing the OAIC's workload. The OAIC could concentrate its efforts on backstop enforcement in cases involving significant misconduct and law violations.
- **Improve compliance**: Certifications may result in improved outcomes and more effective compliance on the ground due to the certification and mandatory periodic re-certification processes and ongoing monitoring requirements, therefore reducing the enforcement burdens of the OAIC.
- **Reduce complaint handling:** Because certifications may include complaint handling and dispute resolution mechanisms, they can help reduce the OAIC's involvement in resolving individual complaints and reserving its involvement for cases involving more serious violations. This aspect of certifications will be important in practice, given that the Privacy Act gives the OAIC a significant complaint-handling role. Moreover, if the OAIC must get involved, formal co-regulatory schemes make enforcement easier as the OAIC can investigate compliance against specific sets of detailed requirements established by certifications and codes of conduct.
- **Transparency**: Certification will require organisations to disclose their data practices in a transparent and organised fashion vis-à-vis the certification bodies and ultimately the OAIC in the event of enforcement. This will make it easier for the OAIC to properly assess these practices as well as possible violations of the relevant requirements. This, in turn, may drive down the costs and burdens of enforcement actions, both for the OAIC and organisations.

In short, such co-regulatory schemes benefit all stakeholders because they put another "cop on the beat" augmenting the capabilities and reach of the OAIC and raising the level of overall privacy protections and compliance. Of course, it is important that such schemes be made affordable and scalable to the size of organisations and the complexity of their processing operations.

D. JOURNALISM EXEMPTION

7. What additional support, if any, would be needed to assist smaller media organisations to comply with privacy obligations?

No comment.

E. ADDITIONAL PROTECTIONS

8. What additional requirements should apply to mitigate privacy risks relating to the development and use of facial recognition technology and other biometric information?

> ***Proposal 13.2:*** *Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities. This work should be done as part of a broader consideration by government of the regulation of biometric technologies.*

CIPL acknowledges the legitimate concerns raised by individuals, regulators, and policymakers regarding the collection and use of biometric data. Requiring robust risk-assessments and implementation of specific risk-based protections and heightened requirements for data uses that involve this type of data could alleviate those concerns. It is important that any laws or rules applicable to biometrics should be careful not to prevent legitimate uses, such as authentication, if the risks can be managed by appropriate mitigations and safeguards. To the extent that Proposal 13.1 requires Privacy Impact Assessments for "high privacy risk activities," CIPL notes that items listed in the Report[16] may not automatically constitutes 'high risk activities' without further assessment of the risks associated with the intended processing. (CIPL is currently working on a white paper about how a risk-based approach to biometric data can enable beneficial and essential uses of such data and will share this paper with the Government in the coming months.)

If policymakers choose to regulate the use of facial recognition technology (FRT) specifically, CIPL encourages them:

- to adopt a risk-based approach that enables beneficial, low-risk uses of FRT while flagging high-risk applications that would be subject to heightened protections. For example, using these technologies for securing access to devices and buildings, or for purposes of authenticating access to banking services, has unlocked conveniences and increased security for individuals while posing lower risks. Moreover, some higher-risk applications may deliver significant benefits if deployed with appropriate safeguards. Thus, it is important to embrace a risk-based approach in order to decide when, where, and how the use of biometrics and facial recognition technology is appropriate.
- to identify specific contexts where FRT would be subject to consultation and authorisation by an appropriate authority—or where FRT would be prohibited outright—considering available safeguards or lack thereof. For example, one might ascribe a high level of risk to real-time applications of FRT by law enforcement versus post-event applications.

[16] Privacy Act Review Report, supra, note 4, section 13.1.2.

F. RESEARCH

9. Should the scope of research permitted without consent be broadened? If so, what should the scope be?

> ***Proposal 14.2***: *Consult further on broadening the scope of research permitted without consent for both agencies and organisations.*

Research is essential for societal progress, and there is some evidence in European countries that data protection rules (or perhaps a misinterpretation of those rules) has had a negative effect on all kinds of research, including scientific, health, and commercial research. Organisations have expressed concern that they are unable to use or share data fully for research purposes, including across borders. This was particularly apparent during the Covid-19 crisis, when there was a need to share personal data and insights for health and vaccine research purposes. It is essential that data privacy rules are conducive to the use of data for beneficial research purposes and that the apparent reticence risk to share data is addressed by the regulators and policy makers.

CIPL supports broadening the scope of research to include all research that benefits and enhances general knowledge and brings benefits and progress for the society and people, including by private sector organisations. As the digitalisation of our society continues and companies invest in new technologies (as well as new and innovative products and services based on those technologies), it is essential that companies be able to create these technologies, products, and services based on extensive research, experimentation, and testing. In fact, the private sector has been investing heavily in internal research functions, and in scientific research, conducted both by academic institutions and in-house research teams.[17] It is essential that companies be able to use data for this beneficial research that ensures that their products and services are built and operate appropriately. For example, training algorithms and AI models to be fair and unbiased can only be done with large and diverse datasets. Companies producing virtual reality hardware or augmented reality software must be able to conduct research with many datasets in the development of their products.

Also, to enable effective research, some of the privacy principles need to be interpreted broadly, such as purpose limitation and restrictions on incompatible processing. Research should be allowed, even if data has not been collected for these purposes.[18] Indeed, the GDPR permits EU member states to provide derogations from some of the data subject rights referred to elsewhere, subject to certain conditions and safeguards.[19]

---

[17] 5 Technology Investing Trends for 2023, Morgan Stanley, Dec 19, 2022, available at https://www.morganstanley.com/ideas/technology-investing-trends-interoperability.

[18] See, for example, GDPR Art.14(5), which provides that certain obligations shall not apply where "the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes …."

[19] See GDPR Art. 89(2): "Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes."

While the AP Review Report only addresses medical research falling within the scope of Art. 95,[20] an accountability-based model could ensure responsible research in other areas with appropriately tailored and proportional protections in a specific context and for a specific purpose.

That said, whether such research should be permitted without consent raises concerns for researchers subject to existing consent obligations under the Privacy Act. If exceptions to the consent requirement are expanded but certain uses of that information still require consent, researchers seeking to use such information may need an appropriate safe harbour exemption.

As mentioned in our response to Question 2, CIPL encourages policymakers in general to consider moving away from the traditional consent model and instead establish an accountability-based model, which places the burden on organisations, not individuals, to prevent harms. This will help deliver stronger protections for individuals. An accountability-based model (1) would provide a range of accountability measures that protect and empower individuals even in the absence of consent, (2) would permit legal bases for processing other than consent; and (3) could enable identification of those circumstances where use of consent is appropriate. Most importantly, placing the onus on organisations to be accountable in their data privacy management practices—especially through the use of risk assessments and risk mitigation measures—is key to protecting individuals from substantial harms.

10. Should there be a single exception for research without consent for both agencies and organisations? If not, what should be the difference in scope for agencies and organisations?

> ***Proposal 14.3***: *Consult further on developing a single exception for research without consent and a single set of guidelines, including considering the most appropriate body to develop the guidelines.*

As noted above in our response to Question 9, CIPL supports broadening the scope of the research exception. And because the principles of organisational accountability are not sector-specific, CIPL does not support a distinction between research by agencies and research by organisations. A contextual risk assessment will determine whether a particular use in a given context will adversely affect different groups of individuals, in different sectors, or in different segments of the economy. Risk assessments also determine whether certain uses are sensitive and high-risk for individuals and, therefore, in need of higher protections (e.g., enhanced security measures, limitations on processing purposes or secondary uses, enhanced transparency, etc.). Such risk assessments should be informed by guidelines that may comprise both general guidance applicable to all research, regardless of sector, as well as additional sector-specific add-on guidance by specialized bodies where useful and appropriate.

[20] Privacy Act Review Report, supra, note 4, section 14.

11. Which entity is the most appropriate body to develop guidelines to facilitate research without consent?

> ***Proposal 14.3***: *Consult further on developing a single exception for research without consent and a single set of guidelines, including considering the most appropriate body to develop the guidelines.*

A single set of high-level guidelines should come from the Office of the Australian Information Commissioner (OAIC), but those guidelines could be supplemented by sector-specific agencies, such as the National Health and Medical Research Council (NHMRC), where sector-specific expertise and guidance is appropriate. As noted in our response to Question 28, CIPL supports regulatory cooperation efforts, such as the **UK Digital Regulation Cooperation Forum** (DRCF)[21] and the **Australian Digital Platform Regulators Forum** (DP-Reg).[22]

G. PEOPLE EXPERIENCING VULNERABILITY

12. What privacy-related issues do APP entities face when seeking to safeguard individuals at risk of financial abuse?

In order to safeguard individuals at risk of financial abuse, APP entities will need to understand their customers and their needs more fully, and to assess their potential vulnerabilities. This may involve the collection of more data than may be strictly necessary for the underlying transaction, and it may also involve the collection of data deemed sensitive and/or confidential in certain contexts. Consequently, policymakers will need to accept and acknowledge these concerns and potential collection practices to enable organisations to do the right thing with confidence as they seek to safeguard individuals at risk of financial abuse.

13. How can financial institutions act in the interests of customers who may be experiencing financial abuse or may no longer have capacity to consent?

> ***Proposal 17.3:*** *Further consultation should be undertaken to clarify the issues and identify options to ensure that financial institutions can act appropriately in the interests of customers who may be experiencing financial abuse or may no longer have capacity to consent.*

Financial institutions should be encouraged to establish best practices and industry standards regarding the identification of vulnerable individuals and their capacity to consent. A contextual risk assessment can help identify the criteria to be used for such evaluations.

Any legal or regulatory approach to addressing the risks of harm (including financial abuse) associated with data processing should focus on enabling an effective risk-based approach to data protection, supplemented with regulatory guidance addressing relevant risk criteria and cognizable harms (including harms associated with the use of financial data), and suggesting appropriate risk-assessment methodologies to be used.

CIPL thus recommends a horizontal approach that includes:

---

[21] The Digital Regulation Cooperation Forum, available at https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum.

[22] Digital Platform Regulators Forum (DP-Reg), available at https://www.acma.gov.au/dp-reg-joint-public-statement.

- a general, principle- and risk-based framework that is comprehensively applicable to all data and data uses;
- co-regulatory mechanisms—such as codes of conduct, certifications, and accountability standards—that translate general rules into specific practices or requirements that can evolve over time; and
- sector-specific industry standards and best practices best suited to the management of customer relationships and the collection of personal data in the given sector.

14. Should the permitted general situations in the Privacy Act be amended to enable disclosure of personal information in safeguarding situations which may not meet the requirements under section 16A, item 1? What other options for reform could be considered to protect people where abuse is suspected while respecting an individual's privacy and personal autonomy?

> ***Proposal 17.3:*** *Further consultation should be undertaken to clarify the issues and identify options to ensure that financial institutions can act appropriately in the interests of customers who may be experiencing financial abuse or may no longer have capacity to consent.*

This question pertains to a concern raised by the Australian Banking Association (ABA). The ABA seeks an amendment to the Privacy Act that permits 'good faith' disclosure of information to law enforcement or adult safeguarding authorities in circumstances when a vulnerable individual's financial safety may be compromised, without a requirement to obtain express consent from such individuals.[23]

CIPL would support an amendment to the Privacy Act that permits 'good faith' disclosure of information to law enforcement or adult safeguarding authorities where vulnerable individuals are at risk. See also our response to Questions 12 and 13, above.

An organisational accountability approach requiring contextual risk assessments would address not only the situation raised by the ABA, but also situations involving vulnerable individuals in other sectors of the economy. Moreover, as noted in our response to Question 2, CIPL encourages policymakers to consider moving away from the traditional consent model and instead establish an accountability-based model, which places the responsibility on organisations to prevent harms as part of how they collect and process customer data. This will help deliver far stronger protections for individuals.

[23] Privacy Act Review Report 2022, supra note 4, section 17.2.3.

H. INDIVIDUAL RIGHTS

15. What would the impact of the proposed individual rights be on individuals, businesses and government?

Proposal 18.1: *Provide individuals with a right to access, and an explanation about, their personal information if they request it, with the following features:*

a. *an APP entity must provide access to the personal information they hold about the individual (this reflects the existing right under the Act)*

b. *an APP entity must identify the source of the personal information it has collected indirectly, on request by the individual*

c. *an APP entity must provide an explanation or summary of what it has done with the personal information, on request by the individual*

d. *the entity may consult with the individual about the format for responding to a request, and the format should reflect the underlying purpose of ensuring the individual is informed, as far as is reasonable, about what is being done with their information*

e. *an organisation may charge a 'nominal fee' for providing access and explanation where the organisation has produced a product in response to an individual*

Proposal 18.2: *Introduce a right to object to the collection, use or disclosure of personal information. An APP entity must provide a written response to an objection with reasons.*

Proposal 18.3: *Introduce a right to erasure with the following features:*

a. *An individual may seek to exercise the right to erasure for any of their personal information.*

b. *An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.*

In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement.

Proposal 18.4: *Amend the Act to extend the right to correction to generally available publications online over which an APP entity maintains control.*

Proposal 18.5: *Introduce a right to de-index online search results containing personal information which is:*

a. *sensitive information [e.g. medical history], or*

b. *information about a child, or*

c. *excessively detailed [e.g. home address and personal phone number], or*

d. *inaccurate, out-of-date, incomplete, irrelevant, or misleading.*

The search engine may refer a suitable request to the OAIC for a fee. The right should be jurisdictionally limited to Australia.

Proposal 18.6: *Introduce relevant exceptions to all rights of the individual based on the following categories:*

a. *Competing public interests: such as where complying with a request would be contrary to public interests, including freedom of expression and law enforcement activities.*

b. *Relationships with a legal character: such as where complying with the request would be inconsistent with another law or a contract with the individual.*

c. *Technical exceptions: such as where it would be technically impossible, or unreasonable, and frivolous or vexatious to comply with the request.*

The PA Review Report proposes new rights to provide individuals with greater transparency and control. Specifically, it proposes:

Rights directed at improving transparency

- Right to access and explanation – a right to know what personal information is held, where it came from, and what is being done with it (including meaningful information about how automated decisions using an individual's personal information are made).
- Right to object to the collection, use and disclosure of personal information – a right to challenge whether an APP entity's handling of information complies with the Act.

Rights directed at giving individuals more control over their information

- Right to erasure – a right to have information deleted.
- Right to correction – a right to require that information be accurate, up-to-date, complete, relevant and not misleading.
- Right to de-index certain search results – a narrow right to have internet search results about an individual de-indexed in specific circumstances.[24]

While CIPL supports the above data subject rights, such rights should not be regarded as unlimited. Boundaries must be set by law and regulations to strike an appropriate balance between protecting the essence of individuals' rights and enabling data uses. These rights must be adapted to increasingly data-driven economies and societies, and take into account new business models, new ways of interacting, predicting or making decisions. Likewise, individuals' rights are not absolute and must be balanced against other fundamental rights such as freedom of expression, the right to conduct a business, protection of trade secrets, as well as legitimate business considerations, such as protection against fraud and security. Finally, these rights must correspond and be proportionate to actual risks of harm and not be merely abstract.

Further, while most individuals exercise their rights in good faith, some individuals and privacy activists consider these rights as unbounded and overwhelm organisations with requests, sometimes for vexatious purposes. Complying with frivolous or excessive requests can be disruptive and resource intensive for organisations.

With clear rules around the exercise of rights in certain circumstances, including limits, organisations can better allocate their resources and prioritise the resolution of legitimate requests. Limitations also help find a balance between data subject rights and other fundamental rights. These limitations should, however, be appropriately balanced so they do not unnecessarily and improperly limit individuals' rights and freedoms, and do not impair individuals' trust in data protection practices.

Specifically with regard to the rights set forth in Proposals 18.1 – 18.6:

- Any requirements regarding the rights to access or correction should apply only if an entity has effective control over the information.
- The proposed requirement to identify the source of any personal information collected indirectly and to provide an explanation could be very onerous on APP

[24] Privacy Act Review Report 2022, supra note 4, section 18.

entities. The 'nominal fee' may be insufficient to recoup costs if requests are made at scale.

- To ensure interoperability, the right to erasure should be consistent with the GDPR. It should be clear that some personal data may be retained if required by law, or for purposes of identity verification, detecting, investigating or preventing fraud or other crime.
- The right to correction should be subject to exceptions for ensuring independent preservation of the version of record and other competing interests, such as where complying with a request directly would be contrary to contractual republishing obligations to the original publisher. Moreover, corrections should be allowed only insofar as it is relevant to the purpose of the data use.[25]
- The right to de-index online search results should be limited to those found on general, public search engines, and subject to countervailing rights such as freedom of expression.
- General exceptions to data subject rights should include competing public interests, such as where complying with a request would be contrary to freedom of expression and information, identity verification, detecting, investigating or preventing fraud or other crime, as well as law enforcement activities.

16. Are further exceptions required for any of the proposed individual rights?

> ***Proposal 18.6:*** *Introduce relevant exceptions to all rights of the individual based on the following categories:*
>
> *a. Competing public interests: such as where complying with a request would be contrary to public interests, including freedom of expression and law enforcement activities.*
>
> *b. Relationships with a legal character: such as where complying with the request would be inconsistent with another law or a contract with the individual.*
>
> *c. Technical exceptions: such as where it would be technically impossible, or unreasonable, and frivolous or vexatious to comply with the request.*

Competing public interests should also include instances of identity verification, along with the detection, investigation, or prevention of fraud or another crime.

Also, there should be general "disproportionate effort" exceptions to transparency requirements and subject access requests, i.e., where providing information or requested access to data would involve an effort that is disproportionate to the benefit of the individual having this information. For example, searching in archived, deleted, or back-up files for information in a response to a subject access request.

[25] APEC Privacy Framework (2015), Privacy Principle VI, available at https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015).

Finally, there should be a general exception where compliance with an individual's right would violate the right of another person, including a legal person.[26]

I. AUTOMATED DECISION-MAKING

17. What types of decisions are likely to have a legal or similarly significant effect on an individual's rights?

> ***Proposal 19.2:*** *High-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Act. This should be supplemented by OAIC Guidance.*

The PA Review Report proposes that entities be required to include information on whether personal information will be used in automated decision-making (ADM) which has a legal, or similarly significant effect on an individual's rights in the entity's privacy policy. The Report further proposes that OAIC guidance should be developed on the types of decisions with a legal or similarly significant effect on an individual's rights.[27]

CIPL believes that adoption of the "legal or similarly significant effects" standard will have significant benefits that are workable and practical for individuals and organisations. First, the standard promotes interoperable solutions for organisations that have to comply with other frameworks such as the Virginia Consumer Data Protection Act,[28] Colorado Privacy Act,[29] Connecticut Data Privacy Act,[30] EU GDPR,[31] UK GDPR[32] (also United Kingdom's draft Data Protection and Digital Information Bill),[33] and Brazil's LGPD.[34] Secondly, reading the standard in conjunction with the risk-based approach addressed above, organisations would bear the responsibility before deploying a new profiling or solely ADM process to identify and mitigate potential risks and harms associated with the covered ADM process. Mitigations could include human review of the ADM. Further, if risk assessments (either during the test phase or subsequent monitoring) show that an ADM tool yields biased results, the organisation should recalibrate the specific ADM model to ensure fair outcomes. The "legal or similarly significant

---

[26] The former UK Data Protection Act included a number of useful exemptions to certain provisions that have generally been seen as reasonable and relevant in many different contexts. See Schedule 7 of the UK Data Protection Act 1998, available at https://www.legislation.gov.uk/ukpga/1998/29/schedule/7/enacted.

[27] Privacy Act Review Report 2022, supra note 4, section 19.3.

[28] § 59.1-573. (Personal data rights; consumers) A(5) of Consumer Data Protection Act, available here.

[29] Section 6-1-1306 (Consumer Personal Data rights) 1(a)(1)(c) of Colorado Privacy Act, available here.

[30] Section 4 (5) Connecticut Data Privacy Act, Senate Bill No 6, Public Act No 22-15 An Act Concerning Personal Data Privacy and Online Monitoring, available here. Please note that Virginia and Colorado privacy rules only allow opt-out rights for profiling in furtherance of decisions that product legal or similarly significant effects concerning the consumer. Thus, there is no opt-out right is provided if profiling not involved even if there is solely automated processing. Nevertheless, Connecticut provides opt out rights limited to solely automated decision-making that result in legal or similarly significant effects.

[31] Article 22 GDPR.

[32] Article 22 of the UK GDPR.

[33] Data Protection and Digital information (No 2) Bill, Article 22A-D, available here.

[34] Article 20 of the Brazilian Data Protection Law (LGPD) Law No 13853/2019, available here.

effects" standard has the benefit of capturing high(er)-risk use cases (e.g. automated processing based on race, gender, health data), while providing greater leeway for automated decisions that do not rise to the level of having legal or similar effects on individuals (e.g. use of training data to build, improve, and enhance algorithms).

Furthermore, it is crucial to have the correct understanding of what constitutes a "legal" effect and a "similarly significant" effect. The concept of "legal effect" is relatively straightforward and can be defined as any impact on someone's rights or something that affects a person's legal status or their rights under a contract. The term "similarly significant" is more difficult. It implies that the effect of a decision based on solely automated processing must be similar in its significance to a legal effect, hence, requiring similar additional safeguards such as data protection impact assessments and appropriately tailored mitigations and redress rights. Although the determination of what constitutes a "similarly significant" effect is highly contextual, the following non-exhaustive criteria could assist in making the determination in cases where it is not clear if the automated decision produces such effects, keeping in mind the high threshold that needs to be reached:

- the duration of impact (temporary vs. permanent) of the automated decision on individuals;
- the severity and likelihood of risks and harms to individuals; and
- the impact of the automated decision at different stages of a decision-making process (i.e. does an initial or intermediary automated decision in a process produce a similarly significant effect or only the ultimate automated decision in that process).[35]

CIPL encourages the OAIC to provide illustrative examples of legal and similarly significant effects and parameters for the threshold to be reached. This will provide clarity and consistency to organisations, especially to be considered during their internal risk assessment procedures. However, organisations should be able to rebut those examples in practice through risk assessments. The table below includes examples on automated decisions producing legal and similarly significant effects.[36]

[35] The UK ICO noted that certain factors may assist in this determination, such as the psychological effects of the decision and whether an individual knows that his or her behavior is being monitored. The Office of the Australian Information Commissioner (OAIC) has commented that the notion of a "similarly significant effect" under Article 22 is quite vague and believes that it should apply in the context of "bigger" decisions. The OAIC believes that some of the current draft privacy legislation in the United States could provide additional clarification in this context. For example, some draft laws propose a non-exhaustive list of "significant effects" which include, denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities and health care services.

[36] This table is based on one provided in our submission to the Article 29 Data Protection Working Party's "*Guidelines on Individual Decision-Making and Profiling*," on December 1, 2017, available here.

CIPL Table on the Application Threshold	
Legal Effects	• Decisions affecting the legal status of individuals; • Decisions affecting accrued legal entitlements of a person; • Decisions affecting legal rights of individuals; • Decisions affecting public rights — e.g. liberty, citizenship, social security; • Decisions affecting an individual's contractual rights; • Decisions affecting a person's private rights of ownership.
Similarly Significant Effects *Some of these examples may also fall within the category of legal effects depending on the applicable legal regime and the specific decision in question*	• Decisions affecting an individual's eligibility and access to essential services — e.g. health, education, banking, insurance; • Decisions affecting a person's admission to a country, their residence or citizenship; • Decisions affecting school and university admissions; • Decisions based on educational or other test scoring – e.g. university admissions, employment aptitudes, immigration; • Decision to categorise an individual in a certain tax bracket or apply tax deductions; • Decision to promote or pay a bonus to an individual; • Decisions affecting an individual's access to energy services and determination of tariffs.
Decisions <u>Not</u> Producing Legal or Similarly Significant Effects *CIPL believes these automated decisions do not typically produce such effects. Instances where they might produce such effects are contextual and should be determined on a case-by-case basis.*	• Decisions ensuring network, information and asset security and preventing cyber-attacks; • Decisions to sandbox compromised devices for observation, restrict their access to or block them from a network; • Decisions to block access to malicious web addresses and domains and delivery of malicious emails and file attachments (e.g. identifying child sex abuse material and content that is objectionable or inappropriate for minors); • Decisions for fraud detection and prevention (e.g. anti-fraud tools that reject fraudulent transactions on the basis of a high fraud score); • Decisions of automated payment processing services to disconnect a service when customers fail to make timely payments; • Decisions based on predictive HR analytics to identify potential job leavers and target them with incentives to stay; • Decisions based on predictive analytics to anticipate the likelihood and nature of customer complaints and target appropriate proactive customer service; • Normal and commonly accepted forms of targeted advertising; • Web and device audience measurement to ensure compliance with advertising agency standards (e.g. requirements not to advertise foods high in fat, sugar and sodium when the audience consists of more than 25 % of children).

When considering proposed laws or regulations on automated decision-making (ADM) systems, policymakers should take the following into account:

- The outcomes intended by some data protection principles (especially data minimisation, retention limitation, and purpose specification) could be achieved by mandating strong accountability-based safeguards, including risk assessments, by organisations collecting, using, and storing the data to enable accurate and fair ADM and a high level of privacy protection for individuals.
- Any laws or regulations should be crafted in consultation with industry, with all stakeholders represented.
- Any laws or regulations should recognise the need to process more data in some ADM contexts (e.g., processing of sensitive data to prevent, detect, and mitigate bias).
- Any transparency requirements should be high-level and principles-based to enable the delivery of appropriate and different forms of transparency for a variety of ADM contexts.
- Any rules on ADM should not prohibit the ability to engage in ADM, but rather focus on ensuring *ex ante* accountability measures and safeguards, including appropriate risk assessments and transparency, as well as appropriate *ex post* redress, including through rights of human review of erroneous or inappropriate automated decisions.

Because the "significance" of a particular application's effect is highly subjective, a risk-based approach to regulating ADM would be essential. Such an approach assesses the risk of the **impact** of ADM technology **in the context of specific uses and applications** rather than the risk of the technology in the abstract. Understanding the potential impact and any risk of harms of a specific ADM application on individuals enables organisations to make risk-based decisions and implement appropriate controls and mitigations to minimise the risks involved in an ADM project. By focusing on impacts and risks, organisations can determine how to allocate resources and ensure appropriate attention is paid to applications that pose higher risks.

Any risk assessment requirement should explicitly include assessing the **benefits** of a proposed ADM application to enable mitigations that, as much as possible, preserve the benefits, or assessing the risks of not proceeding with the development or deployment of the application (i.e., reticence risk).

After conducting a risk assessment for specific ADM applications, organisations may find that the residual risk level is still too high. In such cases, organisations should have the possibility to consult with the OAIC regarding the application, revise the scope of the ADM project to reduce the risks or abandon the project and consider alternatives. Australia's regime should leave such assessments and determinations to organisations as they will be best placed to holistically assess the risks involved. Of course, under the accountability principle, organisations must be able to demonstrate their risk assessments and decision-making process on request by an appropriate regulator for enforcement purposes. Moreover, this flexible approach will ensure that Australia's regime can apply universally to all ADM applications.

For additional information, see CIPL's *Top Ten Recommendations for Regulating AI in Brazil*,[37] as well as CIPL's *Recommendations on Adopting a Risk-Based Approach to Regulating Artificial Intelligence in the EU*.[38]

18. Should there be exceptions to a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made? (Please select one.) Please provide examples of what these exceptions should be.

> *Proposal 19.3: Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect.*
>
> *This proposal should be implemented as part of the broader work to regulate AI and ADM, including the consultation being undertaken by the Department of Industry, Science and Resources.*

☒ Yes

☐ No

☐ Unsure

The ability to explain is an essential principle for developing trustworthy automated decisionmaking models. In line with the U.S. National Institute of Standards and Technology's Four Principles of Explainable AI,[39] CIPL recommends that the OAIC avoid requiring organisations to provide overly detailed descriptions of complex algorithms behind automated decisionmaking processes. This is particularly important to ensure that organisations can provide "meaningful" information to average consumers about the underlying automated decisions and its logics. Full transparency of algorithms (i.e. disclosure of source code or extensive descriptions of the inner workings of algorithms) is not meaningful to users and does not advance their understanding of how their data is being handled in ADM processes.

In addition, consumer access rights must be balanced with organisations' legitimate interests in protecting their trade secrets, intellectual property rights, and similar types of commercially sensitive information that would be put at risk through detailed disclosure requirements. For

---

[37] *CIPL's Top Ten Recommendations for Regulating AI in Brazil*, October 4, 2022, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[en]_cipls_top_ten_recommendations_for_regulating_ai_in_brazil__4_october_2022_.pdf.

[38] *CIPL Recommendations on Adopting a Risk-Based Approach to Regulating Artificial Intelligence in the EU*, March 22, 2021, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_risk-based_approach_to_regulating_ai__22_march_2021_.pdf.

[39] The National Institute of Standards and Technology prescribes the following principles for explainable AI systems: (i) explanation – a system delivers or contains accompanying evidence or reason for outputs and/or processes, (ii) meaningful – a system provides explanations that are understandable to the intended consumers, (iii) explanation accuracy – an explanation correctly reflects the reason for generating the output and/or accurately reflects the system's process, and (iv) knowledge limits – a system only operates under conditions for which it was designed and when it reaches sufficient confidence in its output. See NIST, "*Four Principles of Explainable Artificial Intelligence*", September 2021, Available here.

example, the provision of information on the logic may prejudice the very purpose of data processing and enable an individual to "game the system" in the future, which would be detrimental to many private and public and societal interests.

Further, if organisations are required to provide information regarding the use of ADM that constitutes a low-risk (e.g. decisions to block access to malicious addresses), it would create unnecessary burdens on organisations and confuse and burden consumers. In that regard, transparency requirements should be both risk-based and principles-based, given that there are countless AI contexts and appropriate transparency may look very different for one AI application when compared with another. A principles- and outcomes-based regulatory approach allows organisations to decide how to achieve the required outcomes through a wide range of contextual mitigations and controls. Meanwhile, the OAIC should encourage organisations to develop best practices for ADM transparency, as part of accountability and responsible and ethical development and use of technology. Finally, the OAIC should take an inclusive approach related to consumer access rights, for instance, by taking into account the needs of non-English speakers or people with inconsistent internet connection so that all residents can seek access information related to the use of high-risk ADM.

J. DIRECT MARKETING, TARGETING AND TRADING

19. What would be the impact of the proposals in relation to direct marketing on individuals, businesses and government?

20. What would be the impact of the proposals in relation to targeting on individuals, businesses and government?

Proposal 20.1: *Amend the Act to introduce definitions for:*

a. *Direct marketing – capture the collection, use or disclosure of personal information to communicate directly with an individual to promote advertising or marketing material.*

b. *Targeting – capture the collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc.) for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class).*

c. *Trading – capture the disclosure of personal information for a benefit, service or advantage.*

Proposal 20.2: *Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes. Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt out.*

Proposal 20.3: *Provide individuals with an unqualified right to opt-out of receiving targeted advertising.*

Proposal 20.6: *Prohibit targeting to a child, with an exception for targeting that is in the child's best interests.*

Proposal 20.8*: Amend the Act to introduce the following requirements:*

a. *Targeting individuals should be fair and reasonable in the circumstances.*

b. *Targeting individuals based on sensitive information (which should not extend to targeting based on political opinions, membership of a political association or membership of a trade union), should be prohibited, with an exception for socially beneficial content.*

Proposal 20.9: *Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals. Consideration should be given to how this proposal could be streamlined alongside the consultation being undertaken by the Department of Industry, Science and Resources.*

The following text responds to questions 19-20:

The right to object or to have an opt-out from direct marketing is included in some other data protection laws, such as the GDPR, and it has become an industry best practice and has been supported by co-regulatory tools provided by the direct marketing industry. CIPL does not object to inclusion of the right to object to direct marketing, as long as it is possible to do this through the provision of an opt-out option or unsubscribe option that can be exercised at any time. Under the GDPR, consent is not required for direct marketing by a first party, as use of data for this purpose can be based on the legitimate interests legal ground for processing. The GDPR includes this clarification in its recitals, and the latest reform of the UK GDPR includes this as an explicit example of legitimate interest processing. In that context, the ability to opt-out is therefore not an example of deemed consent, but rather the implementation of a right

to object to direct marketing that can be exercised at any time. A similar approach would make sense in Australia.

The proposals on targeting should be carefully considered with respect to impacts on the ad-supported services ecosystem, and to ensure that they do not unduly restrict service customisation and personalisation that are largely beneficial for consumers. Furthermore, digital marketers in Australia may face competitive disadvantages compared to the counterparts in countries with less prescriptive regulations, making it harder for them to compete for global customers and grow their businesses. Moreover, personalisation is the way by which many services will be provided in the near future, by both public and private sector organisations, including the health sector (e.g., from personalised medicine to personalised recommendations and personalised content). "Targeting" and personalisation will also increasingly be used to ensure online safety and provide age-appropriate content to all individuals, including children. Many age verification solutions also depend on targeting and personalisation.

Also, clarification is needed regarding how an individual's right to opt-out would work in relation to targeted advertising that relies on de-identified or unidentified information, particularly where such information consists of aggregated insights based on a large sample of consumers. Moreover, it is not obvious why there should be a right to opt out to the extent that the use of data and the impact on individuals does not create risks and harms.

Additionally, further clarity is required about how the redefined term 'personal information' will interact with the proposals on targeted advertising.

The OAIC should provide guidance on whether the fair-and-reasonable standard mentioned in Proposal 20.8 could be met without requiring consent.

Finally, regarding Proposal 20.6 on rules for targeting to children, again, it is critical to understand how targeting and personalisation can promote the best interests of the child, which is the growing global standard for considering how to protect and enable children in the digital environment. It provides a more balanced approach and includes many rights and interests, including the right to education, information, freedom of expression, safety, as well as privacy. Targeting and personalisation must be allowed where they are in the best interests of the child, specifically to protect their online safety, to provide age-appropriate content, to enable age assurance methodologies, and to provide appropriately tailored educational resources. The OAIC should work with industry and other relevant regulators to create a framework to consider the best interests of the child, including the risks and benefits from the processing of personal data, and to consider use cases on what constitutes targeting and/or direct marketing that is in the child's best interests.

CIPL further recommends the use of regulatory sandboxes on these topics to discover best practices related to targeting, direct marketing, and methods of personalisation.

21. What would be the impact of the proposals in relation to sale of personal information on individuals, businesses and government?

> ***Proposal 20.1:*** *Amend the Act to introduce definitions for:*
>
> *a. Direct marketing – capture the collection, use or disclosure of personal information to communicate directly with an individual to promote advertising or marketing material.*
>
> *b. Targeting – capture the collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc.) for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class).*
>
> *c. Trading – capture the disclosure of personal information for a benefit, service or advantage.*
>
> ***Proposal 20.4:*** *Introduce a requirement that an individual's consent must be obtained to trade their personal information.*
>
> ***Proposal 20.7:*** *Prohibit trading in the personal information of children.*

If the government chooses to adopt Proposal 20.4 and require consent for any "trading" of personal information, the government will need to clarify whether such consent will be opt-in or opt-out.

Moreover, the government should provide exceptions for data sharing purposes involving the detection, investigation, or prevention of fraud and other crimes; for purposes of identity verification, due diligence, "know your customer" (KYC), or other screening and legal compliance activities; and for purposes of other risk management activities. This type of sharing cannot be considered a disclosure of personal information for a benefit, service, or advantage, even though there are clear benefits and advantages for the disclosing organisation, others in the ecosystem, and wider society from such data sharing.

CIPL recommends further consultation on use cases that would require opt-in consent as opposed to opt-out consent, and how risk assessments can help determine where opt-in or opt-out consent is required. In all cases, regardless of whether opt-in or opt-out, all instances of trading personal information should be subject to the full range of appropriate accountability measures, including transparency, robust risk assessments, and mitigations.

Without opining on whether consent should be required, CIPL would like to highlight that a consent requirement could interfere with activities that are in the public interest. Personal information is often disclosed between entities for the purpose of fraud prevention and ensuring the security of payment systems. Due to the highly sophisticated technology needed to parse through an extraordinarily large amount of information, entities of all sizes commonly outsource fraud prevention and related services.

Data is crucial to the effective and efficient functioning of financial services, and in modern financial services the volume of data is enormous. According to the Reserve Bank of Australia, in 2021/22 Australians made around 650 electronic transactions per person on average.[40] It must be remembered that the majority of these transactions are done online. According to Australian Payments Network, online card fraud now accounts for 85% of all fraud on

[40] The Evolving Retail Payments Landscape | Payments System Board Annual Report – September 2022 | RBA, available at https://www.rba.gov.au/publications/annual-reports/psb/2022/the-evolving-retail-payments-landscape.html.

Australian cards, therefore combatting card-not-present (CNP) fraud remains a key focus for financial institutions and card schemes.[41]

The analysis of financial data for fraud prevention purposes is beneficial not only to Australian consumers, but also to the Australian Government. Lower fraud incidence means that fewer resources are expended by merchants, banks, and governments for investigating and prosecuting fraudulent transactions. Lower fraud incidence would also allow Australian consumers to trust the use of digital payments.

22. Are there any technical or other challenges you would face in providing information about how your algorithms target users to provide them with online content or recommendations?

> ***Proposal 20.9:*** *Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals. Consideration should be given to how this proposal could be streamlined alongside the consultation being undertaken by the Department of Industry, Science and Resources.*

See our response to Question 18.

CIPL supports a general requirement to provide notice to users so that they are aware of why they are getting certain recommendations. Indeed, this is already a best industry practice and there are many ways in which businesses inform users (e.g., "Why am I seeing this ad?" and "Why am I receiving this information?") in both just-in-time notices and privacy policies. However, this should be kept to general information that is actually useful to individuals, as opposed to detailed information about the workings of an algorithm. Individuals are far less likely to find such detailed information useful, and there may be also concerns over disclosing commercially sensitive information, trade secrets, and/or intellectual property rights.

CIPL understands that transparency also means transparency to regulators, and companies should be able to explain to regulators on request (as part of an investigation or a complaint) how their algorithms work and how recommendations are made. Otherwise, there should not be a proactive requirement to provide this information to regulators in every instance. That would be too burdensome for both organizations and regulators. Lastly, it is important that confidential commercial information about algorithms is adequately protected. There should be guardrails in the legislation to prevent inappropriate sharing of such information.

[41] Cards | Australian Payments Network, available at https://www.auspaynet.com.au/network/cards.

23. Please share any examples of situations where greater transparency about how individuals are being targeted by recommender algorithms is not necessary or important to individual or societal wellbeing.

> ***Proposal 20.9:*** *Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals. Consideration should be given to how this proposal could be streamlined alongside the consultation being undertaken by the Department of Industry, Science and Resources.*

This question demonstrates why contextual risk assessments are essential. A risk assessment would help determine whether a particular use in a given context would require greater transparency. The greater the impact of the algorithms, the more important it is to provide appropriate user-centric and understandable information about it, including about relevant redress options.

There are certain use cases where it is clear that the use of recommender algorithms is unlikely to result in significant harms for individuals—for example, recommendation engines used routinely in shopping for certain household goods. In the long term, it will be impractical to require such transparency for all use cases. In fact, individuals will increasingly understand how these operate, and personalisation and recommendation engines may not require explanation to the same extent that they do today.

K. SECURITY AND DESTRUCTION

24. What baseline privacy outcomes should be included in APP 11?

> ***Proposal 21.2:*** *Include a set of baseline privacy outcomes under APP 11 and consult further with industry and government to determine these outcomes, informed by the development of the Government's 2023-2030 Australian Cyber Security Strategy.*

CIPL agrees that the proposed amendment to APP 11.1 should clarify that "reasonable steps" to protect information from misuse, interference, and loss should include "technical and organisational measures." As CIPL supports an **outcomes-based approach**, CIPL supports a proposal to identify expected outcomes under APP 11, to be drafted after engagement and discussions with stakeholders. Alignment with international standards (such as found in GDPR Art. 32) is recommended. One outcome should be to ensure that any data protection measures and safeguards be proportional to the risks and benefits; over-regulation in areas where there is low risk may preclude legitimate data uses, and under-regulation in areas where there is a high risk could fail to protect individuals.

Furthermore, the security provisions must also explicitly refer to and encourage the adoption of industry standards to help operationalise and provide best practices in the data security domain.

25. What are the barriers APP entities face to minimise collection and retention of identity credential information (e.g. reference numbers from, or copies of, drivers' licences and passports)?

> ***Proposal 21.6:*** *The Commonwealth should undertake a review of all legal provisions that require retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information.*
>
> *This further work could also be considered by the proposed Commonwealth, state and territory working group at Proposal 29.3 as a key issue of concern where alignment would be beneficial.*
>
> *However, this review should not duplicate the recent independent review of the mandatory data retention regime under the Telecommunications (Interception and Access) Act 1979 and the independent reviews and holistic reform of electronic surveillance legislative powers.*

Notwithstanding the Australian Government Digital Identity System, which purportedly removes the need for retention of identification documents, data may have already been extracted from traditional forms of identity credential information. While traditional data protection principles of data minimisation and purpose limitation are clearly aimed at providing better privacy protections, these principles are increasingly in tension with modern technologies such as AI and blockchain. Continued adherence to these principles without careful consideration of their application to new technologies may undermine substantial benefits and innovations, negatively impacting the digital economy and society.

Access to large amounts of data potentially collected for a different purpose is critical to building analytics models, AI systems, and machine learning algorithms. AI systems in particular need diverse data sets, including sensitive data, to understand and subsequently limit biased and discriminatory outputs. Notwithstanding the data minimisation and purpose limitation principles, it can be difficult to know ahead of time what is "necessary" in the AI context, since the processing of more and more data may lead to new discoveries and correlations, may maximise the accuracy of results, and may improve bias detection and prevention. Moreover, AI technology has the capability of finding new and beneficial uses for old data (e.g., in the financial industry, old data can reveal patterns and identify trends that were unknown at the time of collection, which can be helpful for fraud prevention).

Again, CIPL recommends the adoption of strong accountability- and risk-based safeguards. A risk-based approach is well-suited to evaluating uses that rely on large volumes of data. It would identify unwarranted risks and adverse impacts, while at the same time permitting legitimate and low-risk processing, without creating automatic barriers for certain forms of data collection and storage that may never raise such risks in the first instance (as may be the case under strict data minimisation and use limitation rules).

L. CONTROLLERS AND PROCESSORS

26. If small business non-APP entities that process information on behalf of APP entities are brought into the scope of the Act for their handling of personal information on behalf of the APP entity controller, what support should be provided to small businesses to assist them to comply with the obligations on processors?

> ***Proposal 22.1:*** *Introduce the concepts of APP entity controllers and APP entity processors into the Act.*
>
> *Pending removal of the small business exemption, a non-APP entity that processes information on behalf of an APP entity controller would be brought into the scope of the Act in relation to its handling of personal information for the APP entity controller. This would be subject to further consultation with small business and an impact analysis to understand the impact on small business processors.*

CIPL would support the implementation of a grace period (e.g., 1-2 years) to allow small businesses time to adopt and implement compliance measures. Further, it would be helpful to develop, or further implement existing, privacy compliance certifications for processors such as the APEC Privacy Recognition for Processors (PRP), which are part of the (soon-to-be global) CBPR system. Through a PRP certification, processors can demonstrate robust data processing capacities in line with common compliance requirements for processors. The certification process can assist processors to come into compliance with relevant APP requirements.

27. Should the extraterritorial scope of the Act be amended to introduce an additional requirement to demonstrate an 'Australian link' that is focused on personal information being connected with Australia?

> ***Proposal 23.1:*** *Consult on an additional requirement in subsection 5B(3) to demonstrate an 'Australian link' that is focused on personal information being connected with Australia.*

The PA Review Report states that the current extraterritorial operation of the Privacy Act (as amended by the Privacy Enforcement Bill) ensures there is sufficient connection with Australia, through the requirement that the entity will need to 'carry on a business' in Australia.[42] The Report proposes that further clarity may be achieved by requiring that foreign organisations or operators must meet the obligations under the Privacy Act if they have an 'Australian link', being:

1. the organisation or operator carries on business in Australia or an external Territory, and
2. the act done or practice engaged in relates to personal information that is *connected to Australia*.[43]

The Report further proposes that the expression 'connected to Australia' would have its ordinary meaning, and could involve consideration of whether:

[42] Privacy Act Review Report 2022, supra note 4, section 23.1.1.

[43] Id.

- the personal information is collected or held in Australia; or
- the personal information is of an Australian or other individual physically located in Australia.

CIPL believes that clarification is needed to ensure that foreign organisations will only be regulated in respect of conduct outside Australia to the extent they are handling information that has been collected in Australia. The OAIC should provide more clarification specifically with respect to personal information collected in other jurisdictions but "held" in Australia., as this data could be subject to conflicting obligations between the laws that apply at the point of collection and Australian law.

28. Should disclosures of personal information to overseas recipients via the publication of personal information online be subject to an exception from the requirements of APP 8.1 where it is in the public interest? How should such an exception be framed to ensure the public interest in protecting individuals' privacy is appropriately balanced with other public interests?

> ***Proposal 23.6:*** *Introduce a definition of 'disclosure' that is consistent with the current definition in APP Guidelines. Further consideration should be given to whether online publications of personal information should be excluded from the requirements of APP 8 where it is in the public interest.*

APP 8.1 provides that before an APP entity 'discloses' personal information to an overseas recipient, the entity must take reasonable steps to ensure the overseas recipient does not breach the APPs in relation to the information. Because the publication of personal information online constitutes an overseas 'disclosure' of personal information, the Report proposes to introduce a definition of 'disclosure' which occurs when an entity makes information accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.[44] If a disclosure is made for purposes of the public interest, an exception to APP 8.1 should require a contextual risk assessment to help identify not only potential harms to individuals but also appropriate protective measures to minimise the risks. It should also balance the public interest in protecting individuals' privacy with other public interests.

M. NOTIFIABLE DATA BREACHES

29. How can reporting processes for Notifiable Data Breaches be streamlined for APP entities with multiple reporting obligations?

> ***Proposal 28.1:*** *Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.*

Given multiple reporting obligations across multiple sectors, it is essential that there be a more streamlined procedure for notifying a single security breach to multiple regulators. Ideally, the requirements for the notification should be the same in all data breach laws, but unfortunately they often are not. Hence, at minimum, regulators should work together to establish a joint notification form, common expectations of information to be provided, and

[44] Privacy Act Review Report 2022, supra note 4, section 23.2.4

the same timeline. In addition, multinational companies have similar obligations in other countries and it would be also important for the OAIC to work with their privacy regulatory counterparts on a common regime for notification of breaches, where possible. The Global Privacy Assembly would be a good platform for such work.

In addition, CIPL endorses regulatory cooperation efforts, such as the **UK Digital Regulation Cooperation Forum** (DRCF)[45] and the **Australian Digital Platform Regulators Forum** (DP-Reg).[46] These are essential initiatives and should be formalised as much as possible, with a set of priorities and joint projects. A streamlined breach notification process across some of the regulators would be an obvious place to start.

The DRCF was formed by the UK data protection regulator (Information Commissioner's Office), the UK competition regulator (Competition and Markets Authority), and the UK communication regulator (Office of Communications) in July 2020. The UK financial services regulator (Financial Conduct Authority) joined the Forum in April 2021.

The DRCF was established to support cooperation between different regulatory bodies to ensure that the digital landscape is regulated effectively, coherently, and efficiently and that regulatory policy is developed in a responsive and holistic way. The DRCF aims to simplify regulation for businesses, reduce regulatory duplications that tend to negatively affect smaller businesses, and engage stakeholders on important conversations.

Australia's DP-Reg brought together the Australian Communications and Media Authority (ACMA), the Australian Competition and Consumer Commission (ACCC), the Office of the Australian Information Commissioner (OAIC), and the Office of the eSafety Commissioner. In June 2022, the four DP-Reg members agreed on a collective set of priorities for 2022–23,[47] but a streamlined breach notification process was not specifically addressed.

CIPL supports setting up a regulatory hub, like DP-Reg, which brings together experts from different regulators to deal with cross-sectoral issues and engage in important discussions. Each regulator keeps its own competence but can exchange views and knowledge, align interpretations, and resolve any areas of conflict. CIPL supports such ongoing joint initiatives and encourages them to develop a streamlined data breach reporting process that works for multiple reporting obligations to different regulators.

[45] The Digital Regulation Cooperation Forum, available at https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum.

[46] Digital Platform Regulators Forum (DP-Reg), available at https://www.acma.gov.au/dp-reg-joint-public-statement.

[47] Digital Platform Regulators Forum names algorithms, digital transparency and increased collaboration as priorities for 2022/23, available at https://www.acma.gov.au/communique-digital-platforms-regulators-forum.

30. Should APP entities be required to take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a Notifiable Data Breach? If so, what factors should be taken into account when determining reasonable steps?

> ***Proposal 28.3***: *Amend subsections 26WK(3) and 26WR(4) to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates.*
>
> *However, this proposal would not require the entity to reveal personal information, or where the harm in providing this information would outweigh the benefit in providing this information.*
>
> *Consider further a requirement that entities should take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach.*

Accountable organisations that have suffered a breach already take corrective action and steps to avoid further breaches and future similar breaches. This is in the interest of the organisations as they work to improve their information security programme and practices and learn from past incidents and security threats. Accountable organisations also strive to reduce the adverse impact of the breach on individuals with appropriate measures.

CIPL supports regulatory guidance to help organisations implement appropriate mitigation measures in the wake of a breach, but the guidance should recommend mitigation measures only for breaches causing actual harm to individuals. In such cases, organisations should take reasonable steps to mitigate such harm and avoid any further harm. Organisations should not otherwise be required to take further steps in relation to individuals (other than internal steps to correct or implement improvements to their systems and processes).

Effective breach reporting rules should serve to protect affected individuals while enabling organisations to operate efficiently as responsible data stewards. It is, therefore, crucial that Australia's approach to breach notification is risk-based and context-specific. The risk-based approach enables organisations and regulators to focus on and allocate their resources to breaches that present the most serious and most likely risks to individuals. The requirements should not be too prescriptive or oblige organisations to implement any specific methodology. Instead, the law and regulatory guidance should include examples of potential risks and harms resulting from various types of incidents, non-exhaustive criteria for assessing the applicable level of risk, or examples of methodologies used for managing incidents.

In addition, organisations should be required to assess the reasonable risk of harm resulting from the breach, considering the state of technology at the time of the breach. Mere speculative considerations or remote possibilities of risks materialising should be explicitly excluded.

It is critical to set appropriate threshold(s) for breach notification to avoid meaningless breach reporting. Defining the threshold according to the number of potentially affected individuals may not be the best approach, as it is not a reliable indicator of the actual harm or likelihood of harm that an individual may suffer as a result of a breach. Further consultation with industry concerning the appropriate reporting threshold(s) would be useful.

Many laws contain a detailed list of the information that must be provided to affected individuals and regulators, such as the nature of the breach, the data affected, when the breach occurred, steps taken to remediate the breach and protect individuals, actions taken to prevent similar breaches from occurring, and the contact information of the notifying organisation. While these may be appropriate categories of information, extensive content

requirements risk overwhelming regulators and affected individuals with useless information, which ultimately reduces the effectiveness of the reporting requirement. Ideally, the law should afford affected organisations discretion to determine what information may be helpful to affected individuals and the regulator, and any additional mitigation.

III. ADDITIONAL COMMENTS

N. PERSONAL INFORMATION, DE-IDENTIFICATION AND SENSITIVE INFORMATION

> ***Proposal 4.6:*** *Extend the following protections of the Privacy Act to de-identified information:*
>
> *• APP 11.1 – require APP entities to take such steps as are reasonable in the circumstances to protect de-identified information: (a) from misuse, interference and loss; and (b) from unauthorised re-identification, access, modification or disclosure.*
>
> *• APP 8 – require APP entities when disclosing de-identified information overseas to take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to de-identified information, including ensuring that the receiving entity does not re-identify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification.*
>
> *• Targeting proposals – the proposed regulation of content tailored to individuals should apply to de-identified information to the extent that it is used in that act or practice. (See further Chapter 20).*

To the extent Proposal 4.6 contemplates that the protections under APP 11.1 should apply to de-identified information, de-identified data may be subject to notification obligations under the Notifiable Data Breaches (NDB) scheme. In the event de-identified data is included as part of the NDB scheme, we strongly suggest that the obligation to notify the regulator or individual should only be where there is (1) a high risk of re-identification of the individual and (2) a likelihood of serious harm to the individual. This will ensure that the notification regime is only triggered in circumstances posing a real risk to the individual and will not result in notification fatigue to the regulator or individuals.

O. ADDITIONAL PROTECTIONS

> *Proposal 13.4: Include an additional requirement in APP 3.6 to the effect that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3.*
>
> *OAIC guidelines could provide examples of reasonable steps that could be taken.*

CIPL broadly supports the position that organisations should ensure that, when obtaining personal information from a third party, the third party complies with the requirements of APP 3. However, we suggest providing clarity on what will constitute 'reasonable steps' for the purpose of this proposal. In particular, we suggest that it would be reasonable for organisations to implement contractual terms to ensure that the third party has complied with the Australian Privacy Principles. In an arm's length commercial transaction, it would be unreasonable to expect organisations to have direct oversight of a third party's collection practices or attempt to intervene in its interactions with consumers. Relevant privacy certifications and codes of conduct could be recognized as appropriate due diligence tools and

"reasonable steps" to ensure that indirectly collected information was collected in compliance with the APP.

P. OVERSEAS DATA FLOWS

> ***Proposal 23.2:*** *Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).*
>
> ***Proposal 23.3:*** *Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities.*

CIPL suggests that OAIC avoid a "white list" approach and instead focus on expanding adoption of mechanisms that focus on upholding the Australian Privacy Principles regardless of jurisdiction. Interoperability mechanisms like the Cross-Border Privacy Rules are especially important for this purpose. In addition, OAIC should clarify that any new measures will operate as alternatives to—but will not invalidate or repeal—existing cross-border transfer mechanisms (such as taking reasonable steps to ensure an offshore recipient does not breach the Australian Privacy Principles in respect of the information transferred—per Australian Privacy Principle 8.1).

IV. CONCLUSION

In sum, any modernisation of Australia's privacy laws should strive for an **outcomes-based approach** that:

- promotes effective, targeted protections for individuals;
- enables innovative and responsible data uses;
- provides businesses with robust, flexible, and future-proof legal bases for processing personal data;
- requires organisations to implement comprehensive organisational accountability and privacy compliance programs that are demonstrable to the OAIC and other relevant regulators on request;
- recognises that risk mitigation does not mean the elimination of risk, but rather the reduction of risk to the extent practicable;
- requires **contextual** risk assessments so that companies may:
    - tailor their compliance measures to their unique risks and use cases;
    - evaluate the sensitivity of data uses and the attendant level of risk in context;
    - identify and prioritise high-risk processing;
    - identify legitimate and beneficial uses of data;
    - evaluate individual, organisational, and societal benefits of data uses;
    - identify appropriate mitigations for a given context and a given use;
    - document their compliance and be able to explain and show their processing decisions under relevant legal standards;
- supports Privacy Enhancing Technologies (PETs) and Privacy Preserving Technologies (PPTs);
- provides guidance on appropriate risk criteria, frameworks, and methodologies;
- takes a reasoned and cautious approach to reliance on affirmative express or opt-in consent and enables opt-out consent where appropriate,
- provides other appropriate legal bases for processing other than consent, and
- is finalised after engagement and discussions with stakeholders.