PrivacyReform@ag.gov.au

Attorney-General's Department
3–5 National Circuit
BARTON ACT 2600

18 September 2026

Electronic Submission via AG website

Dear Privacy Reform team,

RE: Privacy Reform – Consultation on Exposure Draft legislation

Electronic Frontiers Australia (**EFA**) and the Australian Privacy Foundation (**APF**) welcome the opportunity to provide comments on the exposure draft of the proposed *Privacy Amendment (Personal Data Protection) Bill 2026* ("**Privacy Amendment Bill**").

Our joint submission is contained in the following pages: It incorporates both new and historical EFA and APF policy shared in previous submissions given and in historical testimony made to the Senate in respect of the reform and modernisation of the *Privacy Act 1988 (Cth*) ("**the Act**").

We have numerous substantive concerns and issues concerning the Bill, in particular its major omissions and the speed with which the government is trying to push this legislation through by what has the characteristics of stifling examination and public debate by providing limited time for drafting submissions and placing a 1,000 word cap on submissions. As such, both EFA and the APF feel that given the importance and criticality of getting privacy reform right, we feel compelled to ensure our detailed views are made available to the public and placed on the record in toto, notwithstanding the coercive control displayed in the submission guidelines.

Australians need a Privacy Act that embraces human rights and rejects the normalisation and democratisation of "*surveillance as a service*" and "*data extraction as a life state*" by Big Tech, Big Business and Silicon Valley oligarchs. This is a golden opportunity for today's government to fix the policy and regulatory privacy missteps of the past 25 years and meet its obligations under its social contract with the Australian people.

Yours sincerely,

John Pane
Chair
Electronic Frontiers Australia

www.efa.org.au

Dr Juanita Fernando
Deputy Chair
Australian Privacy Foundation

www.privacy.org.au

About EFA

Established in January 1994, EFA is a national, membership-based, not-for-profit organisation representing Internet users concerned with digital freedoms and rights.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political, and civil liberties issues involved in the use of digital communications systems.

About the APF

The Australian Privacy Foundation has been Australia's leading public interest voice in the privacy arena since 1987.

The APF is the nation's foremost independent civil society body concerned with community data protection, privacy and information security expectations. The APF is supported and advised by a panel of notable Australians, and worldwide luminaries including former judges and former Ministers of the Crown.

The APF leads the fight to defend the right of people to control their personal information and to be free of needless intrusions. The APF continues to draw government attention to human privacy rights issues in submissions to parliamentary committees and government agencies.

Acknowledgement of country

EFA and the APF acknowledge Aboriginal and Torres Strait Islander peoples as custodians of Australia and pay our respects to Elders, past and present. We also acknowledge the ongoing connection to land, sea and communities throughout Australia, and the contributions they make to the lives of all Australians

Statement on the use of Artificial Intelligence

All arguments, legal positions, and policy recommendations contained within EFA and APF submissions are the product of human labour encompassing direct research, synthesis, and review of human policy/subject matter experts, board members, and, as applicable, qualified volunteers.

Contact

EFA: Chair@efa.org.au

APF: juanita.fernando@privacy.org.au

Submission on Privacy Amendment (Personal Data Protection) Bill 2026

1. Preliminary Comments

Electronic Frontiers Australia (**EFA**) and the Australian Privacy Foundation (**APF**) welcome the opportunity to provide feedback on the *Privacy Amendment (Personal Data Protection) Bill 2026* (**Bill**).

Whilst recognising numerous positive improvements afforded by the Bill, we believe this reform package continues to sustain entrenched policy flaws of successive Australian governments since 1988 when the Privacy Act was first enacted. That is, from a rights standpoint, this Bill continues to treat privacy largely as a consumer protection or risk management issue rather than a fundamental, non-derogable human right.

EFA and the APF are partially supportive of the Bill as it is currently drafted. It's a good start but more must be done to wrest the locus of power from Big Tech and the tentacles of their surveillance based data extractive business model and provide better, human rights based privacy protections for Australian citizens.

We are however both disappointed with the short time frame for submissions and accompanying word cap/limitation at 1000 words. Both of these requirements give rise to a substantial injustice when considering the significance of the Bill, the failure of the Privacy Act - despite its so called 'technological neutrality' - to keep pace with and solve advances in technology and the broad range of problems and serious power asymmetry between Big Tech, Big Business and citizens.

We advocate for Privacy by Default, not Privacy by Design. The policy differences between the two are not subtle nor nuanced, further structural reform and policy change is required. It is essential that the government adopts key EFA and APF recommendations for further reform by uplifting the Bill or otherwise committing to a further Tranche III of reform. Such additional Privacy Act reform must be predicated on establishing equivalency and alignment with human rights-based privacy laws such as the *General Personal Data Protection Regulation 2018* **(GDPR)** in the European Union 2018 and *Personal Information Protection Act 2020* (**PIPA**) in South Korea. This additional body of policy of work will go some way in dealing with the numerous issues overlooked by the government and identified in submissions from EFA, APF and other digital rights and civil society groups' pertaining to the Bill.

For the reasons given above and also as laid out below in our response, EFA and APF are unable to commit to the incredibly short response limit of 1000 words set by the Attorney-General's department. Jointly, EFA and the APF are concerned by the numerous substantive issues regarding the Bill and its significant omissions. We are compelled to ensure our views are shared and recorded on the public record.

Australians need a Privacy Act that embraces human rights and rejects the normalisation and democratisation of "surveillance as a service" and "data extraction as a life state" by Big Tech, Big Business and Silicon Valley oligarchs. This is a golden opportunity for today's government to fix the policy gaps and regulatory privacy missteps of the past 25 years and meet its obligations under their social contract with the Australian people.

2. Executive Summary

The Attorney-General's Privacy Act Review Report (**2023 Report**), published in February 2023 following several years of consultation, put forward 116 proposals to reform Australia's privacy framework.

The Government's first step was the introduction of the 'Tranche 1' reforms, contained in the *Privacy and Other Legislation Amendment Act 2024*. Tranche 1 dealt with 23 of the proposals, including a statutory tort for serious invasions of privacy, a tiered penalty regime, doxxing offences, and the groundwork for a Children's Online Privacy Code.

Tranche 2 was intended to address the remaining proposals the Government had agreed to implement. The Draft Bill encompasses **some, but not all**, of the proposed Tranche 2 reforms.

The review of the Privacy Act has been ongoing since 2019. The temptation to rush it to a close now laden with many gaps and unnecessary legacy exemptions **must be resisted.** The passage of this Bill without an accompanying promise from the government to fully commit to a further Tranche III reform package or major uplifts to the Bill would be a serious failure by the government to uphold its duty of care to all Australians under its social contract by failing to recalibrate the power asymmetry that exists between Big Tech and Australian citizens.

Public sentiment has finally caught up to arguments made by privacy advocates, civil liberties groups and academics for years: there is irrefutable evidence that online tracking, profiling and targeting are driving a range of digital harms across our community, affecting adults and children alike. The latest data from the Privacy Commissioner's *Australian Community Attitudes to Privacy Survey* (**ACAPS**) results show that 78% of Australians don't feel like they have real control over how their personal information is collected and used.

From a human rights perspective, maintaining legacy exemptions built on flimsy logical foundations and omitting other important privacy uplifts denies baseline privacy protections to citizens in their day-to-day lives, in their workplaces and in electoral participation.

Whilst recognising numerous positive improvements afforded by the Bill, EFA and the APF firmly believe this reform package continues to sustain the entrenched policy flaws of successive Australian governments since 1988 when the Privacy Act was first enacted. From a rights standpoint, this Bill continues to treat privacy largely as a consumer protection or risk management issue, rather than a fundamental, non-derogable human right.

EFA and the APF are partially supportive of the Bill as it is currently drafted. It's a good start but more must be done to wrest the locus of power from Big Tech, Silicon Valley and their surveillance-based data extractive business model to create and provide better privacy protections for Australian citizens.

3. Recommendations

EFA and the APF make the following recommendations. In Part 1 we make recommendations for historical issues and continuing privacy risks which can be resolved by uplifting this Bill or in a subsequent Bill as part of a Tranche III privacy reform Bill. In Part 2 we make recommendations that are pertinent to the provisions of the proposed Bill following the format of the Consultation Paper.

Recommendations Part 1

EFA and the APF recommend:

1. The removal of the Employee Records Exemption and in its place include a specific and tightly drafted Permitted General Situation to deal with situations that cause a serious conflict with employers' rights or obligations under other laws.

2. The removal of the Small Business Exemption without qualification.

3. The remainder of the Political Party Exemption be removed without qualification.

4. That the Privacy Act specifies the mandatory designation of a Data Protection Officer for regulated entities, scalable in line with the relevant size of the regulated organisation or entity. We **further recommend** the OAIC provide guidance to organisations and agencies on the minimum designation, skills, experience, education and professional qualifications of a Data Protection Officer.

5. Introducing strict, human rights-preserving laws to regulate the use of biometric and facial recognition software technologies based on and equivalent to EU laws - namely, the GDPR 2018 and the AI Act 2024. We **further recommend** that a moratorium be placed on the further deployment of biometric and FRT software applications in public spaces until an appropriate, human rights-preserving legal framework is constructed.

6. A direct right to object to data processing be granted to individuals via an active, enforceable mechanism to halt automated profiling, behavioural inference generation, or third-party data sharing on an individual basis.

7. The creation of a Direct Right of Action for Individuals, to provide a remedy for privacy harms suffered which fall outside the scope of the current statutory tort for a serious breach of privacy.

8. A legal obligation be created to mandate the undertaking of a PIA by all APP regulated entities for “high risk privacy projects” in alignment with the Privacy (Australian Government Agencies – Governance) APP Code 2017.

9. The enactment of a federally enforceable Australian Human Rights Act or Charter of Rights. EFA and the APF have been lobbying for this legislation for close to **two decades** now.

10. The Handling Personal Information provisions obligations for regulated entities to deal with the outstanding algorithmic transparency and fairness requirements not covered by the Privacy and Other Legislation Amendment Act 2024 are included in the Bill and, further include an obligation for entities to explain decisions that significantly affect individual’s rights.

Recommendations Part 2

EFA and the APF recommend:

11. The definition of **collects** should include a qualifier such as "*irrespective of how long the personal information is stored or processed*" to preclude similar arguments from being raised as per the Bunnings case and the issue of "*data retention*" being measured in seconds or fractions thereof.

12. The definition of **consent** must be amended to include the principle of "*capacity*" to ensure children and vulnerable people are protected.

13. The definition of **personal information** and Section 6FD, Note 1 of the Bill should be amended to include a new sub-section Note (1) (f) to specifically include technical information or device information as a basis upon which a person may be identified or is considered to be reasonably identifiable.

14. The fair and reasonable test contained in Schedule 1, Section 3.2 of the Bill must be amended to include two other qualifications:

    a. The collection of personal information must be subject to a threshold that is '**strictly necessary**' to achieve the purposes of processing;

    b. The collection of personal information should then be subject to a formal data minimisation and purpose limitation test to determine whether the threshold has been met or not.

15. The proposed APP 5.3 notice be amended by including a new limb at 5.3(e) which reads: "*(e) conspicuous, prominent and easy to find*" and that any hypertext links used to deliver a collection notice require mandatory click through from consumers.

16. The opt out mechanisms given under APP 7.4 be updated to include new sub-clause (e) which provides "*opt out mechanisms must be conspicuous, prominent and easy to find".*

17. Updating APP 11.1 to include new sub-clause 11.2 which says: "*When assessing the appropriate level of security which is reasonable in the circumstances, entities must account for the risks presented by processing that personal information type, specifically focusing on accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.*"

18. Introducing a new sub-clause 11.2.1 which says: "*To evaluate the risks inherent in their processing activities and implement mitigating measures, entities must consider, at a minimum, the following security protection mechanisms:*

    a. The pseudonymisation and encryption of personal data.

    b. The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.

    c. The ability to restore availability and access to personal data in a timely manner following a physical or technical incident.

    d. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures.

e. *Reasonable resourcing of a cyber security or information security function within the entity.*

f. *The creation of a Personal Information Inventory; and*

g. *The creation of a Record of Processing Activities for personal information.*"

19. APP 11.2 be amended to ensure personal information is destroyed or de-identified on the earlier of the completion/cessation of the reason for which it was collected or twelve months (12), unless a longer retention period is required by applicable law.

20. Clause 12.3A provisions be tightened to limit the exception to circumstances where providing access by entities is technologically impossible or subject to another lawful exception.

21. Schedule 4, Part 2 of the Bill be amended to include a mandatory right of erasure for individuals based on language which is equivalent to the EU principles of Grounds for Erasure contained in Article 17(1) of the GDPR and the Statutory Exceptions further made under Article 17(3) of the GDPR.

22. Schedule 6 of the Bill be amended to include provisions creating a legal obligation for entities to use model contractual terms, developed jointly by the Office of the Information Commissioner and the Attorney-General's department, and which are consistent with Article 28 of the GDPR.

23. The OAIC is allocated additional funding and increased long term resourcing to adequately provide guidance, community outreach and education, and to support efficacious and timely regulatory compliance and enforcement activities.

4. Important Omissions which must be restored

The Bill has failed to solve the following privacy risks and harms. These are not novel issues and in some instances have existed for over 20 years. **Now is the time to fix them**.

4.1 Employee Records Exemption

EFA and the APF hold the view that the collection, use, disclosure, transfer and storage of employee personal information must be treated no differently than other types of personal information, including sensitive information. Employee personal information must be subject to the same fundamental definition as personal information, be subject to GDPR-like collection limitation and proportionality, purpose specification and use limitation principles and protections.

In light of the special relationship between an employer and its employees, including the typical 'imbalance of power' that naturally arises, EFA and the APF consider the protection of personal data held in employee records of particular importance. The current regulatory anomaly where an individual applying for employment with an organisation has a range of privacy rights in connection with their employment application but can immediately lose those privacy rights and protections the minute they become an employee of an organisation is an untenable human and privacy rights gap.

Since 2000 advances in technology have normalised and democratised the growing prevalence of novel, intrusive and/or surreptitious surveillance techniques – such as keystroke tracking, collection of biometric data, computer usage monitoring software, wearable trackers, neurotechnology and artificial intelligence. These pose risks and significant harms to worker privacy and undermine workers' trust in their relationships with employers. The current rush by employers to adopt AI technologies only serves to increase these risks and harms and must be contained.

The logical and demonstrable equivalence between employee personal information and other personal information types is clearly reflected in the commonality of the informational typologies, technologies and platforms upon which all personal information is processed and stored, including third party infrastructure and systems residing in foreign jurisdictions. In view of these facts, employees are clearly subject to the same privacy risks and harms as other individuals whose personal information is collected, processed and stored by organisations and agencies.

EFA and the APF are of the firm view that both public and private sector employees, and by inference all employee personal information collected or created by organisations and agencies, should be subject to the same rights and protections as all other individuals under the Privacy Act.

The employee records exemption is an indefensible anomaly that strips individuals of their fundamental human rights the moment they sign an employment contract. It must be completely repealed to ensure workers are protected against unchecked surveillance and undisclosed data breaches. Any legitimate conflicts with HR operations – such as managing misconduct investigations or health and safety – do not justify blanket exemptions. Instead, these specific edge cases should be managed by creating an employment-specific "*Permitted General Situation*" under the Act.

EFA and the APF recognise that as part of the exemption's removal, there may be a need to make minor adjustments to the rights of access and correction in respect of employee personal information to mirror the circumstances reflected by the current Australian Privacy Principles which, in the context of the employer-employee relationship, should continue to be both relevant and workable.

EFA and the APF recommend the removal of the Employee Records Exemption and in its place include a specific and tightly drafted *Permitted General Situation* to deal with situations that cause a serious conflict with employers' rights or obligations under other laws.

4.2 Small Business Exemption

EFA and the APF strongly support the removal of the small business exemption as it has created an extraordinarily large gap in privacy protections for Australians over a significant period - since the introduction of the inadequate National Privacy Principles in 2001.

The small business exemption (which applies to businesses with an annual turnover under $3 million) does not protect a fringe minority of the economy; **it exempts the vast majority of it.** According to recent Australian Bureau of Statistics (**ABS**) data, there are over 2.7 million actively trading businesses in Australia. Small businesses account for between 97.3% and 98% of all Australian businesses. This means an estimated 2.5 million businesses operate entirely outside the federal privacy framework. Public expectation is fundamentally misaligned with this legal reality. Research from the OAIC shows that 85% of respondents mistakenly believed small businesses were covered by the Privacy Act.

We appreciate some small businesses may lack the capabilities to implement the new requirements of the Privacy Act and this can be overcome by the development of implementation guidance, information sheets and outreach from the OAIC – a model used in numerous foreign jurisdictions, e.g., the Information Commissioner's Office – United Kingdom.

Removing the small business exemption is necessary because privacy is a universal human right, not a consumer protection metric tied to corporate revenue. "Turnover" is not a valid proxy for privacy and other legal risks. Revenue size does not correlate with technical capability or personal information ingestion volume. A technology startup, boutique real estate agency, social media influencer, or specialised health clinic with a turnover well under $3 million often process thousands of highly sensitive records, including biometric, financial, health and precise geolocation data.

A proliferation of invisible covert algorithmic profiling has occurred since 2000. The barrier to entry for advanced analytics and automated decision-making (ADM) systems has lowered significantly during this time. Small businesses can now routinely deploy algorithmic profiling, targeted tracking, and AI-driven capabilities – all resulting in the collection of more personal information and consequentially increasing cyber and information security risks relating to its storage and processing. Without strong privacy protections, these severe risks will continue to grow without the prophylaxis effect afforded by strong, human rights-focused privacy law.

Australia's small business exemption under the Privacy Act 1988 must be repealed because it excludes approximately 98% of Australian business entities from baseline data protection standards. This regulatory blind spot legally permits millions of businesses to operate with impunity in their handling of personal information. Combined with rising cybercrime costs – now averaging $56,600 per incident for small businesses – and the unchecked ingestion of customer data into AI tools and social media platforms have resulted in the collection of siloes of fragmented personal, sensitive and private data about people.

The siloes of information contains millions of 'honey pots', all stored under different data management systems, sometimes proprietary in nature, pose a significant data security threat. The small business exemption, and consequent data fragmentation problem, present a systemic threat to national cybersecurity, requiring an immediate and unequivocal improvement to privacy rights and protections for all Australians.

EFA and APF recommend the removal of the Small Business Exemption without qualification.

4.3 Political Party Exemption

The ‘political party’ exemption is both an anachronism and fundamental failure of public policy by successive Federal governments since 1988. It must be removed completely with no carve-outs.

Modern political parties are now fully immersed in the digital world and are completely data driven. They collect vast troves of personal information on citizens and constituents, often without their knowledge or consent and augment these information stores by purchasing more personal information from third party data brokers, whose collection practices are far from transparent and fair (the provisions of this Bill notwithstanding).

Removing the political exemption under the Privacy Act is critical because the unregulated harvesting and micro-targeting of voter data undermines democratic integrity. Political opinions are sensitive human rights data, and allowing political entities to operate shadow surveillance and influence systems without transparency or accountability erodes the foundational principle of a secret ballot and fair elections. Looking at the practices of other jurisdictions, political parties are not exempt from the General Data Protection Regulation 2018. They are classified as data controllers and are subject to strict regulatory requirements when collecting, storing, or using personal data.

The political party exemption creates a severe conflict of interest and undermines public trust when the lawmakers responsible for regulating the digital economy, mitigating cyber threats, and enforcing corporate data protection standards explicitly exempt themselves and their own organisations from those exact same obligations. Registered political parties therefore must unequivocally be treated as if they were organisations and be subject to the same obligations made under the Privacy Act without exception.

EFA and the APF recommend the remainder of the Political Party Exemption be removed without qualification.

4.4 Organisational Accountability - Appointment of Data Protection Officer

Amending the Privacy Act to mandate the appointment of a Data Protection Officer (**DPO**) is a necessary structural safeguard. It shifts organisational privacy from a reactive compliance exercise to a proactive governance framework, ensuring that a dedicated, independent voice represents individual data rights within corporate decision-making structures.

Privacy compliance for private sector organisations is often decentralised or treated as a secondary duty for legal or IT departments. Mandating a DPO ensures there is an identified executive responsible for privacy outcomes, structural accountability, and embedding "Privacy by Design" into product development and corporate strategy.

EFA and the APF recommend that the Privacy Act specify the mandatory designation of a Data Protection Officer for regulated entities, scalable in line with the relevant size of the regulated organisation or entity.

EFA and the APF further recommend the OAIC guides organisation and agencies on the minimum designation, skills, experience, education and professional qualifications of a Data Protection Officer.

4.5 Biometrics and Facial Recognition Technology

Australia's existing privacy framework, designed before the advent of automated biometric surveillance, treats facial recognition primarily as a data management issue rather than an encroachment upon a fundamental human right. And because biometric templates are immutable they cannot be reset if compromised. Currently,no regulatory framework minimises this systemic risk at the architectural level..

The Privacy Act currently relies heavily on the premise that individuals can meaningfully consent to the collection of their sensitive information. In the context of facial recognition technology (**FRT**) deployed in public spaces, retail environments, or transport hubs, consent is neither informed nor voluntary. Providing notice via store signage – as seen in the regulatory actions against major Australian retailers such as Bunnings and Kmart – forces individuals to choose between surrendering their biometric data or being excluded from essential services and public life. This type of consent is legally flawed and is not human rights-preserving.

New laws are required to shift the burden of accountability from the individual's "consent" to tighter tests being required to assess whether the use of biometrics and FRT can be executed in a way that is compatible with human rights and the preservation of privacy in both private and public spaces.

To adequately protect digital and human rights, EFA and the APF recommend that Australia should implement a purpose-built, rights-preserving regulatory framework for biometrics and FRT that combines the strict data protection principles of the EU General Data Protection Regulation (GDPR) with the structural, risk-based prohibitions of the EU Artificial Intelligence Act (AI Act). This approach shifts the regulatory burden from individual consent to systemic accountability for data controllers in the private and public sectors.

Such legislation would establish that certain applications of technology are fundamentally incompatible with human rights and must be banned entirely, regardless of technical accuracy. Australia should therefore adopt equivalent EU statutory prohibitions to establish hard legal limits on surveillance and narrow, legislatively and judicially approved exemptions

We need legislation that categorically prohibits real-time remote biometric identification in publicly accessible spaces with limited exceptions granted via judicial authority. The law must also prohibit the untargeted harvesting of facial images from the internet or CCTV footage to construct facial recognition databases. For biometric applications that are not prohibited (such as biometric verification for secure access control or device unlocking), Australia should adopt the AI Act's "High-Risk" classification model.

EFA and the APF recommend regulating the use of biometric and facial recognition technology using human rights-preserving laws modelled on the EU General Data Protection Regulation 2018 and the EU Artificial Intelligence Act 2024. EFA and the APF also recommend that a moratorium be placed on the further deployment of biometric and FRT software applications in public spaces until an appropriate, human rights-preserving legal framework is constructed.

4.6 Right to Request Cessation of Processing

Australia's privacy framework lacks a general statutory right for individuals to demand the cessation or restriction of data processing, contrasting with Articles 18 and 21 of the EU GDPR. Establishing this right is a necessary structural mechanism to ensure individual data autonomy, control secondary, unrelated data uses, and allow for the suspension of processing during disputes.

The Privacy Act currently limits the right to cease processing to direct marketing communications in certain circumstances. A more general right to object is required to allow individuals to halt data processing based on an entity's internal corporate interests or secondary functional uses without having to terminate their use of the service entirely.

EFA and the APF recommend a direct right to object to data processing be granted to individuals via an active, enforceable mechanism to halt automated profiling, behavioural inference generation, data subject tracking or third-party data sharing on an individual basis.

4.7 A Direct Right of Action

The current statutory tort for a serious invasion of privacy sets the legal threshold too high to address everyday corporate data mishandling. Because the tort requires proof of "intentional or reckless" conduct, it effectively excludes negligent data breaches and other routine but consequential Australian Privacy Principle (**APP**) violations. The tort also lends itself to being more readily available to individuals with strong financial resources. It is exclusionary to individuals who are vulnerable or have limited resources financially.

The statutory tort as it currently stands requires an invasion of privacy to be intentional or reckless. It does not cover negligence. The majority of mass data breaches result from corporate negligence - such as failing to secure databases, misconfiguring servers, deliberate unauthorised access/disclosure/use of personal information by employees or contractors or ignoring patching schedules in violation of APP 11. Without a direct right of Action, individuals have no direct legal avenue to seek damages from a company that carelessly exposes their personal information.

The statutory tort however is designed to address highly offensive, targeted privacy violations (e.g., voyeurism, doxxing, revenge porn) where the conduct meets the high bar of being objectively "serious." A direct right of action is therefore necessary to address systemic, everyday breaches of the APPs - such as deceptive consent models, over-collection of personal data, or failing to delete data at the end of its lifecycle. These structural violations may not meet the high "serious" threshold embodied in the tort, but they still erode digital rights and can result in completely avoidable privacy harms.

EFA and the APF recommend the creation of a Direct Right of Action for Individuals, to provide a remedy for privacy harms suffered which fall outside the scope of the current statutory tort for a serious breach of privacy.

4.8 Mandatory Privacy Impact Assessment (PIA)

A Privacy Impact Assessment (**PIA**) protects individuals by forcing organisations to systematically map, analyse, and mitigate privacy risks before a project is launched. PIAs operationalise "Privacy by Design," as they ensure that they help identify and mitigate privacy risks, facilitate privacy compliance and ensure human rights safeguards are all structurally embedded into a system’s architecture.

For standard commercial businesses, tech companies, and non-profits (defined as "organisations" under the Privacy Act), conducting a PIA is currently a highly recommended best practice, but it is not an all encompassing regulation. Further, while *Australian Privacy Principle (**APP**) 1.2* requires entities to take "reasonable steps" to implement privacy compliance practices, the Office of the Australian Information Commissioner (**OAIC**) cannot currently compel a private organisation to conduct a PIA under general circumstances.

Current private sector legal obligations are in stark contrast to obligations for public sector agencies arising under the *Privacy (Australian Government Agencies – Governance) APP Code 2017* where Commonwealth agencies **must** conduct a written PIA for all "high privacy risk projects."

EFA and the APF recommend that a legal obligation is created to mandate the undertaking of a PIA by all APP- regulated entities for "high risk privacy projects" in alignment with the Privacy (Australian Government Agencies – Governance) APP Code 2017.

4.9 Federally Enforceable Human Rights Act

EFA has **for over 20 years**, strongly advocated for the enactment of a federally enforceable Australian Human Rights Act or Charter of Rights. EFA's foundational stance is that digital rights are human rights, and a national charter of human rights is necessary to provide a legally binding baseline that protects privacy, freedom of expression, and civil liberties in the digital age. This perspective is **strongly supported** by the APF. It is an important part of restoring equilibrium and social licence between the powers of Big Tech and government and the rights of individuals.

EFA has consistently stated in its parliamentary submissions that Australia is the only Western liberal democracy without a national human rights act. EFA views this legislative absence as a structural vulnerability that helps normalise and democratise pervasive surveillance, data extraction, and government overreach to occur without adequate constitutional or statutory checks.

EFA and the APF submit that specific technology regulations, such as the Privacy Act or the Data Availability and Transparency (DAT) Act, operate in a vacuum without an overarching rights framework. A national Human Rights Act would mandate that all technology policy and legislation be drafted, interpreted, and audited against established human rights principles.

Pending the introduction of a federal human rights act or charter, EFA and the APF advocate for interim measures requiring rigorous Human Rights Impact Assessments (**HRIAs**) for any legislation or government project involving extensive data sharing, biometric surveillance, or automated decision-making.

EFA and the APF recommend the enactment of a federally enforceable Australian Human Rights Act or Charter of Rights.

4.10 Impacts of AI/AI Agents and Algorithmic Transparency and Fairness

While the Bill's broadened definition of 'collects' covers AI-generated inferences, there are no standalone obligations governing AI systems, agentic AI, or automated decision-making beyond the transparency requirements already enacted in the *Privacy and Other Legislation Amendment Act 2024* (commencing 10 December 2026).

The Bill has further omitted obligations that require entities to explain substantially automated decisions that significantly affect individuals' rights. The Bill does not build on the basic transparency obligation in the 2024 Privacy Act amendments.

EFA and the APF recommend the Handling Personal Information provisions obligations for regulated entities to deal with the outstanding algorithmic transparency and fairness requirements not covered by the Privacy and Other Legislation Amendment Act 2024 are included in the Bill and, further includes an obligation for entities to explain decisions that significantly affect individual's rights.

EFA and the APF recommend the Bill's Handling Personal Information provisions obligations for regulated entities to deal with the outstanding algorithmic transparency and fairness requirements not covered by the Privacy and Other Legislation Amendment Act 2024 and further include an obligation for entities to explain decisions that significantly affect individuals' rights.

5. Departmental Questions

5.1 Are the proposed updated definitions sufficient to address the risks of emerging technologies?

No. Emerging technologies such as facial recognition technology (**FRT**), AI and wearable devices such as Meta style 'smart glasses' are the latest evolutionary step of Big Tech's surveillance-based data extractive business model that the purportedly "technologically neutral" National Privacy Principles and later Australian Privacy Principles, were designed to provide a bulwark against.

The proposed changes to the definition of 'personal information' or 'collect' will not mitigate against the harms to individuals being surveilled in circumstances where there is a reasonable expectation of privacy or later where these images and data are uploaded to third party organisations like Meta and their ad tech partners for potential data subject identification (via biometrics and FRT), followed by exploitation and monetisation. Other harms may still arise even when the identity of an individual is not reasonably ascertainable by the user and embarrassing, body shaming or intimate imagery can be shared online via social media platforms and messaging/chat groups.

5.2 Is the definition of 'collection' sufficiently flexible to capture information collected via new technologies such as wearables?

No. While the expansion of the definition of 'collection' is welcome, it is not sufficient to cover the use of wearables by individuals uploading third party personal information and then sharing that data with third party data controllers or processors such as Meta and their Ad Tech partners.

5.3 To what extent can the reforms ensure that consent is meaningful, given that wearable technologies compromise the transparency of captures and uses of individuals' personal information?

The Privacy Act and the new Bill primarily regulate entities, not individuals acting in a personal capacity. If a wearer records a bystander and keeps the footage on their device or personal computer, the Privacy Act does not apply. When personal information is uploaded to corporate servers (e.g., Meta), the "notice and consent" model fails because bystanders cannot realistically provide informed consent to a roving device. In public spaces, consent is meaningless.

Smart glasses and wearable surveillance devices fall within clear structural gaps existing in Australia's privacy and surveillance laws. This is because they shift data collection from regulated entities to individual citizens. Our current laws fail to adequately address this **corporate outsourced, covert, roving surveillance data extractive business model**. It requires legislative reform beyond the current Bill to modernise surveillance data and device definitions, impose hardware-level privacy-by-design mandates, and prohibit real-time biometric processing.

5.4 Are existing remedial options adequate, including to ensure that individuals whose privacy has been interfered with can seek removal of relevant content? If not, what additional measures should be considered (without duplicating existing powers)?

No. Remedial options are centred around often opaque action taken by regulators. Individuals, as complainants, are limited to the capacity of those organisations such as the Office of the Information Commissioner (**OAIC**), to handle complaints in a timely manner.

We know from OAIC data that complaint resolution is often severely protracted due to chronic under-resourcing of the Privacy Commissioner's Office. In addition, recent comments from the Privacy Commissioner regarding the toughening of complaint acceptance thresholds do not bode well for those individuals who have suffered privacy harms as the result of wearable surveillance devices.

A Direct Right of Action may go some way in ameliorating harms attributable to covert surveillance, but this places the responsibility on the aggrieved party to initiate and bear costs - which can give rise to undesirable outcomes, especially for vulnerable or financially constrained individuals.

5.5 To what extent will the existing or proposed measures encourage improved compliance?

The "fair and reasonable test" will most likely result in extending the scope, duration and harms caused by the existing Privacy Act's structural problem. **We need a legislative solution that prevents the normalisation and democratisation of "surveillance as a service" and "data extraction as a life state" for Big Tech, Big Business and Silicon Valley oligarchs while facilitating human rights and life improving use cases of these devices, e.g. for sight impaired individuals.**

The use of biometrics and FRT should generally be a prohibited use case in line with Section 4.5 of our submission. To fix this issue EFA and the APF recommend:

5.5.1 Harmonisation of Surveillance Laws:
State and federal surveillance device laws must be unified and updated to explicitly regulate body-worn optical and audio sensors, removing the reliance on physical trespass as a threshold for optical recording offences.

5.5.2 Mandatory Privacy-by-Default Hardware Standards
Legislation should mandate physical safeguards for wearable cameras sold in Australia. This includes hard-wired recording indicators (e.g., LEDs that cannot be disabled via software) or physical shutters, ensuring bystanders have environmental awareness.

5.5.3 Prohibition on Real-Time Biometric Identification
Aligning with risk-based frameworks like the EU AI Act and the GDPR, Australian law should explicitly prohibit the integration of real-time facial recognition technology into consumer wearable devices, classifying such use as an unacceptable human rights risk.

5.5.4 Imposition of a Digital Duty of Care
Hardware manufacturers and platform operators must be required to proactively identify and mitigate systemic risks associated with their devices, rather than shifting the burden of privacy protection entirely onto the individual wearer or the bystander.

6. Schedule 1 - Core Definitions

EFA and the APF are generally aligned with and supportive of the new definitions proposed in the Bill with the following exceptions:

6.1 Collects

The amended definition would provide that an entity collects personal information when it includes that information in a record or generally available publication, regardless of the source from which, or means by which, the information is obtained.

EFA and the APF recommend that the definition includes a qualifier such as "*irrespective of how long the personal information is stored or processed*" to preclude similar arguments from being raised as per the Bunnings case and the issue of data retention measured in the seconds or fractions thereof.

6.2 Consent

The definition mirrors existing guidance and interpretation that consent must be voluntary, informed, current, specific and unambiguous. However, it is inexplicably silent on capacity, calling into question what this means for children and vulnerable people.

EFA and the APF recommend that the definition of consent be amended to include the principle of "capacity" to ensure children and vulnerable people are protected.

6.3 Personal information

The proposed definition of personal information needs additional clarity, particularly around the concept of "individuation" and the relevance of technical or device information and its place in facilitation technology based individuation.

EFA and the APF recommend that the definition of personal information and Section 6FD, Note 1 of the Bill should be amended to include a new sub-section Note (1) (f) to include technical information or device information as a basis upon which a person may be identified or is considered to be reasonably identifiable.

7. Schedule 2 - Handling of Personal Information

7.1 The Fair and Reasonable Test for the Collection of Personal Information.

EFA and the APF are partially supportive of a **fair and reasonable test** as an additional protection but we do not support the proposed replacement of established statutory constraints with a standard that gives entities greater discretion in determining what is fair and reasonable.

The Bill sets out seven non-exhaustive factors to determine whether the handling of personal information is fair and reasonable in the circumstances, which are:

- reasonable expectations of the individual
- connection to the entity's functions or activities
- transparency
- whether the purpose for handling could be met by collecting less information (data minimisation)
- whether the individual was given a genuine choice in relation to the handling
- the impact on the privacy of the individual and the proportionality of such impact
- in the case of a child, to consider their best interests.

The Consultation Paper states that an entity would not be required to satisfy every legislated factor for a collection, use or disclosure to be fair and reasonable. It also states that no single factor is determinative and that the factors must be considered holistically. These principles provide limited guidance on how competing factors should be weighed or what weight should be given to each. For example, EFA and the APF believe that the '*reasonable expectations of the individual*' and '*the impact on the privacy of the individual and the proportionality of such impact'* must be mandatorily assessed and receive a strong weighting favouring the objects of the Privacy Act: "*To promote the protection of the privacy of individuals with respect to their personal information and to recognise the public interest in protecting privacy."*

The Bill does not go far enough in protecting an individual's privacy rights. In its current form, the proposed fair and reasonable framework risks weakening privacy protections, would be difficult to apply consistently, and would continue to rely predominantly on enforcement after harm has occurred rather than stronger ex ante accountability and oversight.

EFA and the APF recommend that the *fair and reasonable test* contained in Schedule 1, Section 3.2 of the Bill be amended to include two other qualifications:

a. The personal information collected must be subject to a threshold that is 'strictly necessary' to achieve the purposes of processing;
b. The personal information collected should then be subject to a formal data minimisation and purpose limitation test to determine whether the threshold has been met or not.

7.2 Notification of the Collection of Personal Information

The proposed obligations in APP 5.3 are insufficient and replicate historical design flaws contained in the Privacy Act and the APPs.

One of the most important factors when deciding whether an organisation has met its 'transparency' and notification requirements should be the conspicuousness, prominence and ease of viewing of the notices it is required to give.

Collection Notices must be a clear and prominent statement articulating the matters they are required to say as simply as possible. Collection notices must not be buried in legal terms and conditions, other texts or hidden in obscure or illegible fonts. Hypertext links which point a user to a collection notice, without forcing a user to click on the link itself, is a serious design flaw that is predicated on consumer inertia by designing a "frictionless experience" (borrowing from the UX/design lexicon of most digital organisations).

EFA and the APF recommend that the proposed APP 5.3 notice be amended by including a new limb at 5.3(e) which reads: "(e) conspicuous, prominent and easy to find" and that any hyper text links used to deliver a collection notice require mandatory click through from consumers.

7.3 Direct Marketing

Organisations frequently rely upon implied or inferred consent in order to engage in direct marketing to individuals. Both the means of consent acquisition by the data controller and consent revocation by the individual are frequently subject to dark pattern design features, making it difficult to opt out of direct marketing communications. Such practices must be prohibited. The Bill will in a small way ameliorate this problem, but it will not entirely fix it.

EFA and the APF recommend that opt out mechanisms given under APP 7.4 be updated to include new sub-clause (e) which provides opt out mechanisms '*must be conspicuous, prominent and easy to find*'.

8. Schedule 3 - Data Security

8.1 APP 11.1 - Security & Destruction of Personal Information

Despite previous Privacy Act Tranche I reforms adding a broad requirement for "technical and organisational measures", data security obligations remain unnecessarily vague and highly discretionary.

The Bill does not mandate specific technical controls such as minimum encryption standards, live data inventories, or verifiable data destruction techniques. Security obligations continue to rely on what entities subjectively deem "reasonable steps," which allows businesses to scale their security investments based on internal risk appetite rather than hard regulatory minimums.

EFA and the APF recommend updating APP 11.1 to include new sub-clause 11.2 which says: " ***When assessing the appropriate level of security or that which is reasonable in the circumstances , entities must account for the risks presented by processing that personal information type, specifically focusing on accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed"*****.**

EFA and the APF further recommend that a new sub-clause 11.2.1 be introduced which says: 'To evaluate the risks inherent in their processing activities and implement mitigating measures. Entities must consider, at a minimum, the following:

(a) The pseudonymisation and encryption of personal data.
(b) The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
(c) The ability to restore the availability and access to personal data in a timely manner following a physical or technical incident.
(d) A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures.
(e) Reasonable resourcing of a cyber security or information security function within the entity
(f) The creation of a Personal Information Inventory; and
(g) The creation of a Record of Processing Activities (**RoPA**) for personal information

Entities must be required to create and maintain an enterprise-wide Record of Processing Activities and Personal Information Inventory. This is a fundamental principle of effective data governance, facilitates effective privacy risk management and assists in the effective and efficient management of data breaches and their remediation.

A **Personal Information Inventory** is the operational mechanism used to discover, classify, and track personal information across systems. It functions as the underlying data source for the RoPA and supports other Privacy Act obligations:

- **Data Subject Rights**: An inventory allows entities to locate specific personal information promptly to fulfil access, rectification, or erasure requests.
- **Security and Breach Notification**: Knowing where personal information resides and its sensitivity level is required to apply appropriate security controls and properly assess the risk of an eligible/notifiable data breach.
- **Privacy Impact Assessments:** The inventory identifies high-risk processing activities that trigger the mandatory completion of a PIA.

- **Record of Processing Activities:** An organisational record that documents specific metadata about an entity's personal information processing activities. This includes the name and contact details of the entity/data controller and Data Protection Officer, purposes of processing, categories of data subjects, categories of personal data, categories of recipients, international data transfers (and specific safeguards used), anticipated retention periods, and a general description of technical and organisational security measures.

8.2 Destruction etc of Personal Information

While the Bill introduces a strict 72-hour deadline for notifying the Information Commissioner of an eligible data breach, it fails to strengthen proactive, prescriptive security baselines that reduce privacy and data breach risks.

Personal information ought not be retained for any period longer than is reasonably necessary to achieve the purpose of its collection or for any other period required by applicable law, e.g. taxation, workplace relations, occupational health and safety laws etc.

Personal information stored for periods longer than what is necessary directly increases privacy and security risks and harms. It also makes unlawful data exfiltration a more compelling business case for bad actors - it creates the well known ‘honey pot’ effect. **See the mega-data breaches involving Latitude Finance, Medibank and Optus.**

EFA and the APF recommend that APP 11.2 be amended to ensure personal information is destroyed or de-identified on the earlier of the completion/cessation of the reason for which it was collected or twelve months (12) unless a longer retention period is required by applicable law.

9. Schedule 4 - Data Access & Erasure

9.1 Data Subject Access Rights

Clause 12.3 A of the Bill creates a carve-out in circumstances where an entity has taken reasonable steps to provide access to personal information but is unable to do so because providing access remains "*unreasonable or impracticable due to technical impossibility*".

From a human rights perspective, a broad statutory carve-out for technical infeasibility risks incentivising non-compliant system architecture. Organisations should not be relieved of human rights obligations because they designed databases that are inherently difficult to audit or query.

EFA and the APF recommend the Clause 12.3 A provisions be tightened to limit the exception to circumstances where providing access by entities is technologically impossible or subject to another lawful exception.

9.2 Data Subject Erasure Rights

The 2023 Privacy Act Review recommended a universal right to erasure for individuals covering all legal entities covered by the Privacy Act. The Bill dilutes this significantly. It restricts the erasure right exclusively to Large Digital Platforms (**LDPs**) meeting a threshold of $500 million in revenue or **2.5 million users**.

LDPs are defined as services covered by the *Online Safety Act 2021* that clear either a $500m gross revenue test or an average of 2.5 million monthly Australian end users. Qualifying platforms would have to destroy personal information on request unless an exception applies, and give written notice identifying what was destroyed, which exceptions were relied on and how to complain

The exceptions are broad, covering law enforcement, retention required by law or court order, technical impracticability, reasonableness, requests that are frivolous or vexatious, and information strictly necessary to deliver an ongoing service to the individual. Data brokers, credit reporting bodies, banks, telcos and retailers fall outside it entirely.

This Bill exempts the vast majority of Australian businesses from complying with deletion requests, leaving most consumers without a statutory mechanism to erase their digital footprint. By doing so it is degrading Australians' human rights and, when considering the scale of additional, non-essential data retention, directly increases information and cyber-security risk from the 'honey pot' effect.

Like the EU, Australians desperately need a universal Right to Erasure (the "*right to be forgotten*") applicable to all data controllers when processing is no longer necessary, consent is withdrawn, or data is unlawfully processed.

The approach proposed in the Bill limits erasure rights to a specific and very small subset of technology companies. This frames privacy as a platform regulation issue rather than a fundamental human right. Individuals are left without statutory mechanisms to enforce digital forgetting against data brokers, retailers, or smaller organisations.

EFA and the APF recommend that Part 2 of the Bill be amended to include a mandatory right of erasure for individuals based on language which is equivalent to the EU principles of Grounds for Erasure contained in Article 17(1) of the GDPR and the Statutory Exceptions further made under Article 17(3) of the GDPR.

10. Schedule 5 - Exception for Research

The rationalisation of the current two exemptions for research (each of which has proven problematic in their own way) is very welcome. For human research projects that are ethically reviewed, approved and monitored in accordance with the National Statement on Ethical Conduct in Human Research, consent would not be required to satisfy the 'current' or 'specific' elements of the definition of "consent". This will help to resolve difficulties many of our public sector clients have faced when they wish to create sources of immense public value for future researchers, such as tissue biobanks and enduring data assets.

11. Schedule 6 - Exception for Information Processors

11.1 Processor and controller framework

To align with privacy frameworks in many other jurisdictions, notably the European Union, the Bill introduces a controller-processor distinction. An APP entity is a 'processor' when it acts in accordance with another APP entity's documented written instructions for purposes specified in those instructions, and the instructing entity is the 'controller'. The definition applies only where both entities are APP entities and excludes contracted service providers for Commonwealth contracts, who remain governed by the existing section 95B framework.

Notably, the Bill does not adopt a previous recommendation from the OAIC regarding mandatory contractual terms modelled on Article 28 of the GDPR, nor does it implement a previous recommendation to bring non-APP entity processors (such as small businesses) into scope when processing on behalf of an APP entity controller.

EFA and the APF recommend that Schedule 6 of the Bill be amended to include provisions creating a legal obligation for entities to use model contractual terms, developed jointly by the Office of the Information Commissioner and the Attorney-General's department, which are consistent with Article 28 of the GDPR.

12. OAIC Powers & Efficiency

The Consultation Paper contemplates measures to enhance the regulatory powers and efficiency of the OAIC, but these are not set out in the draft Bill. These are proposed to cover:

- privacy complaint making and handling processes, including making privacy complaint handling compliance for entities mandatory and enforceable;
- representative complaint processes;
- assistance obligations and strengthened information gathering processes for the OAIC; and
- clarified Ministerial reporting powers.

EFAand the APF strongly recommend that the OAIC be allocated significant additional funding and increased long-term resourcing to adequately provide guidance, community outreach and education, and give effect to efficacious and timely regulatory compliance and enforcement activities.

13. Addressing Emerging Technologies

The "technology neutral" design of the Australian Privacy Principles (APPs) was intended to future-proof the Privacy Act 1988, but instead, has enabled Big Tech, Ad Tech and Social Media Platforms to leapfrog ahead of the law and create an enforcement vacuum that structurally fails to map to modern digital ecosystems. By relying on broad, analogue concepts - such as whether data is strictly "about" an identified or reasonably identifiable individual or collected for inclusion in a "record" - the framework permits tech companies to exploit semantic loopholes. An example of this is data brokers and ad tech firms that weaponise device fingerprinting and Mobile Ad IDs, arguing that such unique identifiers relate to a browser rather than a natural person, thereby leaving mass individuated tracking entirely unregulated (a privacy wrong which this Bill will hopefully solve).

Because the law refuses to mandate specific technical mechanisms or structural bans, it provides no defense against automated, continuous passive surveillance. The APPs' reliance on a linear notice-and-consent model completely breaks down against the realities of Real-Time Bidding, where data is auctioned to unseen third parties in milliseconds. Furthermore, tech-neutrality fails to recognise that the mere act of public biometric scanning – such as deploying facial recognition technology in retail spaces to map crowds in real-time – is inherently privacy and human rights invading, even if no permanent "record" is stored. Similarly, the framework fails to impose "Privacy by Default" principles on wearable devices, allowing them to continuously harvest highly sensitive physiological telemetry and biometric data without meaningful regulatory friction and necessary limitations and restrictions.

To successfully future-proof the *Privacy Act 1988* without resorting to rigid, quickly outdated technological definitions, the law must shift from a procedural, tick-box framework (how data is collected) to an outcomes-based, rights-centric framework (the impact of the processing). In addition, specific privacy framed, rights-based laws must be developed for the specific use cases of biometrics and facial recognition technology. Such laws should be human rights protecting and at least equivalent to European Union laws such as the *General Data Protection Regulation 2018* and the *Artificial Intelligence Act 2024*.

14. Closing Statement

Whilst recognising numerous positive improvements afforded by the Bill, EFA and the APF believe this reform package continues to sustain entrenched policy flaws of successive Australian governments since 1988 when the Privacy Act was first enacted. **From a rights standpoint, this Bill continues to treat privacy largely as a consumer protection or risk management issue rather than a fundamental, non-derogable human right.**

EFA and the APF are partially supportive of the Bill as it is currently drafted. It's a good start but more must be done to wrest the locus of power from Big Tech and their surveillance-based data extractive business model and provide better privacy protections for Australian citizens.

To make this law better, fairer and stronger EFA and APF recommendations 1 – 23 should be adopted to ensure the Privacy Act aligns with human rights principles such as those adopted in the European Union and their data protection, Artificial Intelligence and digital market regulation laws.

Beyond updating definitions and introducing a fair and reasonable test and other actions proposed by this Bill, future-proofing the Privacy Act requires dismantling the structural power imbalances between Big Tech platforms and users. This is achieved by democratising enforcement through a direct right of action, explicitly outlawing "dark patterns" in interface design, introducing broad data deletion rights, removing archaic exceptions and shifting the regulator from a reactive, complaints-driven body to a proactive enforcement agency with robust auditing powers.

Australians have been waiting since 1988 for a Privacy Act that embraces privacy as a human right and rejects the normalisation and democratisation of "*surveillance as a service*" and "*data extraction as a life state*". This is a golden opportunity for today's government to fix the structural policy and regulatory privacy missteps of the past 25 years and meet its obligations under its social contract with the Australian people by treating privacy as a non-derogable human right to protect Australians against the predacity of Big Tech, Big Business and silicon valley oligarchs. The government needs to remember "*privacy = digital rights = human rights*" and must be legislated as such.

John Pane
Chair
Electronic Frontiers Australia Inc.
www.efa.org.au

Dr Juanita Fernando
Deputy Chair
Australian Privacy Foundation
www.privacy.org.au

END