Privacy Act Review
Attorney-General's Department
PrivacyActReview@ag.gov.au

10 April 2023

By Email

Dear Attorney-General,

RE: Report on Review of the Privacy Act - 02/2023

EFA welcomes the opportunity to make a submission on the Report on the Review of the Privacy Act issued by the Attorney General on 23rd February 2023. We also thank the Attorney General's office for granting EFA an extension until April 10, 2023 to make its submission.

This is EFA's third submission in connection with the Attorney General's review of the *Privacy Act 1988 (Cth)* and builds upon EFA's prior substantial submissions of 26 November 2020 and 10 January 2021.

Our submission is contained in the following pages.

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 communication and information systems.

Yours sincerely,

John Pane
Board Member
Electronic Frontiers Australia

Kathryn Gledhill-Tucker
Vice Chair
Electronic Frontiers Australia

1. Objects of the Act

Proposal 3.1 *Amend the objects of the Act to clarify that the Act is about the protection of personal information.*

EFA holds the view that the proposed objects of the Act continues to send a clear and unacceptable message that while privacy is finally receiving some moderate recognition as an human right which benefits individuals, families, communities and society in the public interest, the requirement for it to be 'balanced' against the ever growing interests and insatiable data appetites of business and its further subordination to what is administratively convenient and expeditious for the government, still falls short of what is required by civil society.

The power imbalance between Big Tech, data platforms, data aggregators and 'surveillance economy' players continue leapfrogging ahead of the law, despite, at least in Australia's case, the use of 'technologically neutral principles' to protect privacy. This power imbalance is even further accelerating due to advances in Algorithmic Decision Systems, Artificial Intelligence, Machine Learning technologies and the hidden, secretive actors of the "Surveillance Economy" who follow our every move on-line and covertly collect and sell our personal information.

EFA proposes the objects of the Act be drafted to expressly state the revised Privacy Act is a human-rights-focused law with strong human rights protection that recognises a right to privacy as being foundational to the public interest in our country.

Proposal 3.2 *Amend the objects of the Act to recognise the public interest in protecting privacy.*

The Privacy Act is human rights law. Accordingly, any interpretation or adaptation of this law is one that best facilitates privacy rights and the protection of individuals from privacy risks. Privacy rights must not be subordinated to government and business interests under a rubric of 'balance' or 'public benefit'.

EFA holds the view that the Act includes a provision expressly stating that when interpreting a provision of the Act, the interpretation that would best achieve the purpose or object of the Act is to be preferred to other interpretations. This will ensure the Government achieves its regulatory principle of 'privacy by default and design'.

4. Personal Information

Proposal 4.1 *Change the word 'about' in the definition of personal information to 'relates to'. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.*

EFA supports proposal 4.1.

Proposal 4.2 *Include a non-exhaustive list of information which may be personal information to assist APP entities to identify the types of information which could fall within the definition. Supplement this list with more specific examples in the explanatory materials and OAIC guidance.*

EFA broadly supports proposal 4.2 but suggests further detailed guidance be given by the OAIC in respect of the collection, classification, use, disclosure and destruction of de-identified personal information, anonymized personal information and the risk of data re-constitution.

Proposal 4.3 *Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.*

EFA supports proposal 4.3 but suggests detailed guidance given by the OAIC in respect of the different means of collection of personal information.

Proposal 4.4 *'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment.*

EFA does not support using the term 'reasonably' identifiable; either an individual is identifiable, or they are not. The harm to privacy from poorly assessed risk of re-identification, both individual and collective, is disproportionate to the subjective assessment of what constitutes 'reasonable' at a specific point in time. What matters is whether or not individuals can be identified, which is an objective standard.

Proposal 4.5 *Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context.*

EFA agrees with the concerns of Associate Professor Vanessa Teague quoted in the Review that 'de-identification for detailed individual records will almost always be re-identifiable'.

EFA supports proposal 4.4 in principle subject to the OAIC providing detailed guidance upon what constitutes 'best available practice' for the de-identification or anonymisation of personal information inclusive of the relative risks between the differing methods to achieve these policy outcomes.

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.

EFA is generally supportive of the proposal to extend APPs 8 and 11.1 to the protection of de-identified personal information subject to detailed guidance from the OIAC as to the types of physical, administrative and technical controls which might be used. Such OAIC guidance should contemplate controls that are relative to the inherent risk of data reconstitution or re-identification based upon the approach used to de-identify the personal information in the first instance.

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.*

EFA strongly opposes this proposal. The risk of data reconstitution or re-identification is more properly managed by the articulation of appropriate guidance and methods to de-identify or anonymize personal information in conjunction with the subsequent application of appropriate administrative, physical and technical controls as currently contemplated by APP 11.1 and Proposal 4.6.

EFA opposes the re-introduction of an amended version of the Privacy Amendment (Re-identification) Offence Bill 2016 and instead proposes that such actions constitute a defined breach of the Privacy Act and separately be regulated by way of statutory tort. See also our response to Proposal 4.8.

Proposal 4.8 *Prohibit an APP entity from re-identifying de-identified information obtained from a source other than the individual to whom the information relates, with appropriate exceptions. In addition, the prohibition should not apply where:*

(a) the re-identified information was de-identified by the APP entity itself - in this case, the APP entity should simply comply with the APPs in the ordinary way.

(b) the re-identification is conducted by a processor with the authority of an APP entity controller of the information.

EFA generally supports Proposal 4.8 provided the 'appropriate exceptions' contemplated by the Proposal are limited to purposes specified in (a) and (b) above and where re-identification is required by applicable law.

Proposal 4.9

(a) Amend the definition of sensitive information to include 'genomic' information.

(b) *Amend the definition of sensitive information to replace the word 'about' with 'relates to' for consistency of terminology within the Act.*

(c) *Clarify that sensitive information can be inferred from information which is not sensitive information.*

EFA submits that 'geo-location data' be included as a class of sensitive information and otherwise supports proposal 4.9.

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.*

EFA partially supports Proposal 4.10 but proposes, consistent with our response to Proposal 4.9, that geolocation data be classified as 'sensitive information', requiring both the express consent of the data subject for its collection, use and disclosure and be subject to GDPR-like collection limitation and proportionality, purpose specification and use limitation principles.

5. Flexibility of the APPs

Proposal 5.1 *Amend the Act to give power to the Information Commissioner to make an APP code where the Attorney-General has directed or approved that a code should be made:*

(a) *where it is in the public interest for a code to be developed, and*

(b) *where there is unlikely to be an appropriate industry representative to develop the code.*

In developing an APP code, the Information Commissioner would:

(a) *be required to make the APP Code available for public consultation for at least 40 days, and*

(b) *be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any stage of the code development process.*

EFA supports proposal 5.1.

Proposal 5.2 *Amend the Act to enable the Information Commissioner to issue a temporary APP code for a maximum 12-month period on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.*

EFA supports proposal 5.2.

Proposal 5.3 *Amend the Act to enable Emergency Declarations to be more targeted by prescribing their application in relation to:*

(a) *entities, or classes of entity*

(b) classes of personal information, and

(c) acts and practices, or types of acts and practices.

EFA supports proposal 5.3.

Proposal 5.4 *Ensure the Emergency Declarations are able to be made in relation to ongoing emergencies.*

EFA supports proposal 5.4.

Proposal 5.5 *Amend the Act to permit organisations to disclose personal information to state and territory authorities under an Emergency Declaration, provided the state or territory has enacted comparable privacy laws to the Commonwealth.*

EFA supports proposal 5.5.

6. Small business exemption

Proposal 6.1 *Remove the small business exemption, but only after:*

(a) an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business - this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act

(b) appropriate support is developed in consultation with small business

(c) in consultation with small business, the most appropriate way for small business to meet their obligations proportionate to the risk, is determined (for example, through a code), and

(d) small businesses are in a position to comply with these obligations.

EFA strongly supports the removal of the small business exemption as it has created an extraordinarily large gap in privacy protections for Australians over a significant period of time since the introduction of the woefully inadequate National Privacy Principles in 2001. No other countries with omnibus data privacy legislation have an equivalent exemption.

EFA appreciates 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.

Proposal *6.2 In the short term:*

(a) prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption, and

(b) *remove the exemption from the Act for small businesses that obtain consent to trade in personal information.*

EFA supports Proposal 6.2 but submits the consent contemplated by Part (b) is express consent.

7. Employee records exemption

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.

EFA partially supports proposal 7.1.

In light of the special relationship between an employer and its employees, including the typical 'imbalance of power', EFA considers 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 immediately loses those privacy rights and protections the minute they become an employee of an organisation is a ludicrous regulatory gap and needs to be fully closed as a matter of urgency.

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, it is clear employees are subject to the same privacy risks as other individuals whose personal information is collected, processed and stored by organisations and agencies.

EFA is 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.

EFA holds 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, and is subject to GDPR-like collection limitation and proportionality, purpose specification and use limitation principles and protections.

EFA recognises that 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 Australia Privacy Principles which, in the context of the employer-employee relationship, should broadly apply.

EFA firmly opposes the construction of a Privacy Code to regulate the processing of employee personal information. There is no compelling logical reason why the management of employee personal information cannot be satisfactorily dealt with by the Privacy Act and supplementary Privacy Principles. Employers and employer lobbyists are often oblivious to the fact that one class of worker is already subject to the protections and rights afforded by the Privacy Act – individual contractors – and the management of their personal information and facilitating their privacy rights is not problematic from any operational, legal or technological perspective.

8. Political exemption

Proposal 8.1 *Amend the definition of 'organisation' under the Act so that it includes a 'registered political party' and include registered political parties within the scope of the exemption in section 7C.*

EFA partially supports Proposal 8.1.

The 'political party' exception 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.

Registered political parties must unequivocally be treated as if they were organisations and be subject to the same obligations made under the Privacy Act without exception.

Proposal 8.2 *Political entities should be required to publish a privacy policy which provides transparency in relation to acts or practices covered by the exemption.*

See EFA's response to 8.1.

Proposal 8.3 *The political exemption should be subject to the following requirements:*

(a) Political acts and practices covered by the exemption must be fair and reasonable.

(b) Political entities must not engage in targeting based on sensitive information or traits which relate to an individual, with an exception for political opinions, membership of a political association, or membership of a trade union.

The political exemption should include a savings clause as per Recommendation 41-2 of ALRC Report 108.

See EFA's response to 8.1.

Proposal 8.4 *The political exemption should be subject to a requirement that individuals must be provided with the means to:*

(a) opt-out of their personal information being used or disclosed for direct marketing by a political entity, and

(b) opt-out of receiving targeted advertising from a political entity.

See EFA's response to 8.1.

Proposal 8.5 *The political exemption should be subject to a requirement that political entities must:*

(a) take reasonable steps to protect personal information held for the purpose of the exemption from misuse, interference and loss, as well as unauthorised access, modification or disclosure

(b) take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for a purpose covered by the political exemption, and

(c) comply with the NDB scheme in relation to an eligible data breach involving personal information held for a purpose covered by the political exemption.

See EFA's response to 8.1.

Proposal 8.6 The OAIC should develop further guidance materials to assist political entities to understand and meet their obligations.

See EFA's response to 8.1.

9. Journalism exemption

Proposal 9.1 *To benefit from the journalism exemption a media organisation must be subject to:*

(a) privacy standards overseen by a recognised oversight body (the ACMA, APC or IMC), or

(b) standards that adequately deal with privacy.

EFA proposes that the current journalism exemption should be abolished and replaced with a limited exemption for media organisations to conduct investigative and public interest journalism. This should be accompanied by detailed guidance, a complaints process (with free external dispute resolution) and sanctions for any breach. All other relevant provisions of the Privacy Act would apply as per those regulating organisations.

Proposal 9.2 *In consultation with industry, and the ACMA, the OAIC should develop and publish criteria for adequate media privacy standards and a template privacy standard that a media organisation may choose to adopt.*

See EFA's response to Proposal 9.1.

Proposal 9.3 *An independent audit and review of the operation of the journalism exemption should be commenced three years after any amendments to the journalism exemption come into force.*

See EFA's response to Proposal 9.1.

Proposal 9.4 *Require media organisations to comply with security and destruction obligations in line with the obligations set out in APP 11.*

See EFA's response to Proposal 9.1.

Proposal 9.5 *Require media organisations to comply with the reporting obligations in the NDB scheme. There will need to be some modifications so that a media organisation would not need to notify an affected individual if the public interest in journalism outweighs the interest of affected individuals in being notified.*

See EFA's response to Proposal 9.1.

10. Privacy policies and collection notices

Proposal 10.1 *Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable. Appropriate accessibility measures should also be in place.*

EFA supports this proposal subject to clear guidance being provided by the OAIC on how to develop these documents with a strong focus on visual design/readability. We take this position because there is an abundance of research establishing both a reluctance of consumers to read these documents due to their size and an inability to understand them when attempting to read them because of the length, complexity and typically arcane legal language used in drafting.

See our further comments under Proposal 10.3.

Proposal 10.2 *The list of matters in APP 5.2 should be retained. OAIC guidance should make clear that only relevant matters, which serve the purpose of informing the individual in the circumstances, need to be addressed in a notice.*

The following new matters should be included in an APP 5 collection notice:

(a) if the entity collects, uses or discloses personal information for a high privacy risk activity —the circumstances of that collection, use or disclosure

(b) that the APP privacy policy contains details on how to exercise any applicable Rights of the Individual, and

(c) the types of personal information that may be disclosed to overseas recipients.

EFA broadly supports this proposal subject to our comments under Proposals 10.1 and 10.3.

Proposal 10.3 *Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.*

EFA strongly supports this proposal and further recommends development of individual style and design guides for the drafting and presentation of privacy policies and notices customised to the relevant method of delivery, i.e., voice recording, paper, audio/visual recording, paper, web and mobile.

11. Consent and privacy default settings

Proposal 11.1 *Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.*

EFA supports Proposal 11.1 subject to:

i. adding the following words to the proposed definition: "…. unambiguous < <u>indication of the individual's wishes through clear action</u>>; and

ii. adding language ensuring that before consent is considered the proposed collection, use or disclosure of the relevant personal information is also subject to the application of GDPR-like collection limitation and proportionality, purpose specification and use limitation principles.

Proposal 11.2 *The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes.*

EFA supports Proposal 11.2 and strongly suggests that further consideration be given to the development of style guides for the acquisition and recording of consent customised to the relevant method of its delivery, i.e. voice recording, paper, audio/visual recording, paper, web and mobile. See further our response to Proposal 10.3 which also impacts upon the drafting and presentation of consent acquisition/revocation mechanisms.

Proposal 11.3 *Expressly recognize the ability to withdraw consent, and to do so in a manner as easily as the provision of consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.*

EFA supports this Proposal and also refers you to our earlier comments at Proposal 11.2.

Proposal 11.4 *Online privacy settings should reflect the privacy by default framework of the Act.*

APP entities that provide online services should be required to ensure that any privacy settings are clear and easily accessible for service users.

'Pro-privacy defaults' ('privacy by design & default' in the EU) are proposed in the Report with two implementation options: (i) pre-set the most restrictive setting required in default; or (ii) easily available privacy settings, with the most restrictive option easy to set. The latter option is clearly not 'privacy by default' and would continue to place the burden – and risk - on individuals to take the necessary steps to protect their personal information from potentially unknown, unwanted and unnecessary uses of their personal information in connection with the relevant product or service which they wish to acquire.

Privacy by Design also correlates to the proposal to limit the collection, use and disclosure of personal information that is proportionate to the primary purpose of collection and directly related to a range of narrow secondary purposes, otherwise known as the privacy critical 'data minimization' and 'purpose limitation' principles under the GDPR.

EFA holds the view that 'privacy by default' should be exactly just that, meaning that the collection of information must be both necessary and proportional to the goal of proposed processing and restricted to the primary purpose of collection and directly related secondary activities. These should be the foundational principles underpinning the development of new, replacement privacy principles under the Privacy Act.

12. Fair and reasonable personal information handling

Proposal 12.1 *Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.*

EFA partially supports this view subject to the inclusion of pre-defined parameters of the reasonableness test which incorporates collection limitation and proportionality, purpose specification and use limitation principles as outlined in our response to Proposal 11.4.

Proposal 12.2 *In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account:*

(a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances

(b) the kind, sensitivity and amount of personal information being collected, used or disclosed

(c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency

(d) the risk of unjustified adverse impact or harm

(e) whether the impact on privacy is proportionate to the benefit

(f) if the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child, and

(g) the objects of the Act.

The EM would note that relevant considerations for determining whether any impact on an individual's privacy is 'proportionate' and could include:

(a) whether the collection, use or disclosure intrudes upon the personal affairs of the affected individual to an unreasonable extent

(b) whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits, and

(c) any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual.

EFA broadly agrees with Proposal 12.2 with the exception of Parts (c) and (e) which need to be re-drafted to:

(c) whether the collection, use or disclosure is necessary for the functions and activities of the organisation or is necessary or directly related for the functions and activities of the agency;

(e) whether the impact on privacy is proportionate to the benefit from the perspective of a reasonable person.

Proposal 12.3 *The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained. The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should not apply to exceptions in APPs 3.4 and 6.2. The reference to a 'fair means' of collection in APP 3.5 should be repealed.*

EFA supports Proposal 12.3 in part. EFA strongly suggests that the 'fair and reasonable' test should apply to all instances of collection, use and disclosure, including where the collection, use or disclosure is authorised by another law, or under an exemption.

13. Additional protections

Proposal 13.1 *APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks.*

(a) A Privacy Impact Assessment should be undertaken prior to the commencement of the high-risk activity.

(b) An entity should be required to produce a Privacy Impact Assessment to the OAIC on request.

The Act should provide that a high privacy risk activity is one that is 'likely to have a significant impact on the privacy of individuals'. OAIC guidance should be developed which articulates factors that may indicate a high privacy risk, and provides examples of activities that will generally require a Privacy Impact Assessment to be completed. Specific high-risk practices could also be set out in the Act.

EFA supports Proposal 13.1.

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 the government of the regulation of biometric technologies.*

EFA supports Proposal 13.2 in principle but strongly suggests the OAIC develop specific guidance for organisations and agencies to assist them with determining the necessity, proportionality and fairness of deploying facial recognition or other biometric systems and the secure processing and storage of biometric data.

Proposal 13.3 *The OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks. Practice-specific guidance could outline the OAIC's expectations for compliance with the Act when engaging in specific high-risk practices, including compliance with the fair and reasonable personal information handling test.*

EFA supports Proposal 13.3.

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.*

EFA supports Proposal 13.4.

14. Research

Proposal 14.1 *Introduce a legislative provision that permits broad consent for the purposes of research:*

(a) Broad consent should be available for all research to which the research exceptions in the Act (and proposed by this chapter) will also apply.

(b) Broad consent would be given for 'research areas' where it is not practicable to fully identify the purposes of collection, use or disclosure of personal or sensitive information at the point when consent is being obtained.

EFA does not support Proposal 14.1. Instead we strongly suggest s.95 and s.95A of the Privacy Act be repealed, and replaced with a single exemption (applicable to APPs 3 and 6), the scope of which includes (as relevant and necessary to each project) the collection, use or disclosure of any types of personal information for research projects in the public interest, including medical research and the activities preceding to or arising from the proposed research activity. The proposed exemption can also prescribe standards for data storage, transfer and de-identification or anonymization.

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

Refer to EFA's response for Proposal 14.1.

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.*

Refer to EFA's response for Proposal 14.1.

15. Organisational Accountability

Proposal 15.1 *An APP entity must determine and record the purposes for which it will collect, use and disclose personal information at or before the time of collection. If an APP entity wishes to use or disclose personal information for a secondary purpose, it must record that secondary purpose at or before the time of undertaking the secondary use or disclosure.*

EFA opposes this proposal. Organisations and agencies 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 more effective privacy risk management and assists in the effective and efficient management of data breaches and their remediation. The requirement to create a Record of Processing Activities and Personal Information Inventory must be a mandatory feature of an integrated, holistic, scalable privacy compliance framework which all organisations and agencies are required to create and maintain under the revised Privacy Act.

Proposal 15.2 *Expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity. This may be an existing member of staff of the APP entity who also undertakes other duties.*

EFA supports this Proposal in principle. EFA strongly suggests that the Privacy Act specify the mandatory appointment of a Data Protection Officer with the OAIC providing guidance to organisations and agencies on the minimum designation, skills, experience, education and professional qualifications of a Data Protection Officer.

16. Children

Proposal 16.1 *Define a child as an individual who has not reached 18 years of age.*

As in previous submissions, EFA strongly urges any legislation to take into account a graduated approach to children's autonomy and decision-making ability. A rigid one-size-fits-all approach based on an arbitrary age limit would be inappropriate.

Proposal 16.2 *Existing OAIC guidance on children and young people and capacity*[1] *should continue to be relied upon by APP entities. An entity must decide if an individual under the age of 18 has the capacity to consent on a case-by-case basis. If that is not practical, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise.*

The Act should codify the principle that valid consent must be given with capacity. Such a provision could state that 'the consent of an individual is only valid if it is reasonable to expect that an individual to whom the APP entity's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.'

Exceptions should be provided for circumstances where parent or guardian involvement could be harmful to the child or otherwise contrary to their interests (including, but not limited to confidential healthcare advice, domestic violence, mental health, drug and alcohol, homelessness or other child support and community services).

Refer to EFA's response to Proposal 16.1.

[1] OAIC, APP Guidelines (July 2019) [B.55]–[B.61].

Proposal 16.3 *Amend the Privacy Act to require that collection notices and privacy policies be clear and understandable, in particular for any information addressed specifically to a child.*

In the context of online services, these requirements should be further specified in a Children's Online Privacy Code, which should provide guidance on the format, timing and readability of collection notices and privacy policies.

EFA supports Proposal 16.3 subject to EFA's earlier response to Proposals 10 and 11.

Proposal 16.4 *Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances.*

EFA supports this proposal subject in principle and subject to appropriate guidance being developed by the OAIC to assist organisations and agencies undertake the fair and reasonable assessment test requirements. OAIC guidance should take account of a graduated approach to children's autonomy and decision-making ability.

Proposal 16.5 *Introduce a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'. To the extent possible, the scope of an Australian children's online privacy code could align with the scope of the UK Age-Appropriate Design Code, including its exemptions for certain entities including preventative or counselling services.*

The code developer should be required to consult broadly with children, parents, child development experts, child-welfare advocates and industry in developing the Code. The eSafety Commissioner should also be consulted.

The substantive requirements of the Code could address how the best interests of child users should be supported in the design of an online service.

EFA broadly supports Proposal 16.5, but has concern for the design and implementation of such a Code. Creating safeguards for vulnerable populations, such as children, introduces its own set of complexities and may lead to broadly damaging the right to privacy of many in the pursuit of safety, particularly with respect to age verification measures. EFA cautions against well-meaning, but technically fraught, desires to protect children's personal information that perversely result in an *increase* in the collection, use, and disclosure of personal information of a population.

EFA submits that privacy and security is a human right for all individuals, not just children, and this should be reflected in legislation.

17. People experiencing vulnerability

Proposal 17.1 *Introduce, in OAIC guidance, a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interference with their personal information.*

EFA broadly supports Proposal 16.5.

Proposal 17.2 *OAIC guidance on capacity and consent should be updated to reflect developments in supported decision-making.*

EFA broadly supports Proposal 17.2

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.*

EFA broadly supports Proposal 17.3.

18. Rights of the Individual

Access and Explanation

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

EFA broadly supports Proposal 18.1.

Objection

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.*

EFA broadly supports Proposal 18.2.

Erasure

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.

EFA supports Proposal 18.3 in respect of limbs (a) and (b) being written into the Privacy Act subject to the removal of the words 'involves disproportionate effort' from (b). An APP entity will ordinarily be storing information in an accessible way.

EFA does not support the proposition that certain, as yet unnamed personal information, should be hived out and stored on the illegitimate basis that 'one day it may be useful for law enforcement purposes'. If there is a particular law enforcement activity that absolutely necessitates organisations and agencies to retain certain types of personal information then this should be enshrined in the relevant law. Agencies and organisations would then be able to rely upon a relevant privacy principle exception for the ongoing storage of this information but with no dispensation or relaxation of their security obligations under the Privacy Act.

We submit that personal information ought not be retained for any period longer than is reasonably necessary to achieve the purpose of the collection or for a period required by applicable law.

We further submit that personal information ought to be deleted on the earlier of the completion or cessation of the reason for which it was collected for twelve months (12), unless a longer retention period is required by applicable law.

Correction

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

EFA supports proposal 18.4.

De-indexing

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.

EFA broadly supports Proposal 18.5.

Exceptions

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.*

EFA broadly supports Proposal 18.6 provided suitable guidance is developed and published by the OAIC to help organisations properly consider the nature of the three exceptions proposed above.

Response

Proposal 18.7 *Individuals should be notified at the point of collection about their rights and how to obtain further information on the rights, including how to exercise them.*

Privacy policies should set out the APP entity's procedures for responding to the rights of the individual.

EFA broadly supports Proposal 18.7.

Proposal 18.8 *An APP entity must provide reasonable assistance to individuals to assist in the exercise of their rights under the Act.*

EFA broadly supports Proposal 18.8.

Proposal 18.9 *An APP entity must take reasonable steps to respond to an exercise of a right of an individual. Refusal of a request should be accompanied by an explanation for the refusal and information on how an individual may lodge a complaint regarding the refusal with the OAIC.*

EFA broadly supports Proposal 18.9 but suggests that it could be amended to include an internal decision review mechanism where individual rights requests are either partially or fully refused.

This will help improve the quality of processing individuals rights requests and will have a measurable impact on reducing enquiries of this type being made to the OAIC.

Proposal 18.10 *An organisation must acknowledge receipt of a request to exercise a right of an individual within a reasonable time and provide a timeframe for responding.*

An agency and organisation must respond to a request to exercise a right within a reasonable timeframe. In the case of an agency, the default position should be that a reasonable timeframe is within 30 days, unless a longer period can be justified.

EFA broadly supports Proposal 18.10 but submits it must be amended to ensure the organisations and agencies are subject to the same obligations for processing individuals rights requests as there is no material distinction between these entities from both a technological or operational perspective that would require such a distinction in processing obligations, or of facilitating an individual's rights request, being made.

19. Automated decision making

Proposal 19.1 *Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights.*

EFA supports Proposal 19.1 in principle subject to our comments on Proposal 10.3.

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.*

EFA supports Proposal 19.2 in principle.

Proposal 19.3 *Introduces a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effects 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.

EFA partially supports Proposal 19.3 in respect of granting individuals a right to request meaningful information about how substantially automated decisions with legal or similarly significant effects are made. Otherwise, this provision remains a policy failure.

Automated decision-making can pose risks for individuals, for instance if the underlying algorithms are 'biased', or simply are not designed to take into account the special

circumstances in which a particular individual finds him- or herself. The need to protect individuals against such risks, in particular through enhanced transparency and 'explainability', has been recognised in international fora like the OECD and G20.

EFA submits that it is critical to include a right in the Privacy Act for individuals negatively affected by decisions based solely or predominantly on automated processing (e.g., rejection of an online credit, e-recruiting, etc.) to at least receive an explanation about the underlying 'logic' of such decisions, to be able to challenge them and obtain their review by a human being.

20. Direct marketing, targeting and trading

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, de identified 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.*

EFA broadly supports Proposal 20.1 and submits strongly that the Privacy Act specifically prohibit the use of 'deceptive design practices' in respect of 'targeting' activities conducted by organisations and agencies.:

Specifically, the Privacy Act must prohibit 'deceptive design practices', also known as 'dark patterns'. Deceptive design practices may be defined as digital interfaces and user journeys implemented on digital platforms, technologies or devices that that actively and surreptitiously attempt to influence and coerce users into making unintended, unwilling and potentially harmful decisions, often toward a decision that is against the users' best interests and in favour of the designers' interests.

Deceptive design practices are a form of digital subterfuge used to facilitate guerrilla marketing, influence human agency and diminish our online sovereignty by weaponizing our online behaviour and personal information against us. It is also a form of digitally stalking someone.

The Privacy Act must be changed to protect individuals from businesses and organisations that stalk, surveil, nudge and shepherd consumers like livestock into an activity or transaction they do not necessarily want to make.

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.

EFA strongly opposes Proposal 20.2. and considers it to be an abject failure of policy. To meet the Government policy intent of creating law that is based on 'Privacy by Default' and 'Privacy by Design' principles, direct marketing should only be allowed to occur with the express consent of the individual. Going back to 2010 there is an abundance of Australian and global research tendered in respect of both the current and past reviews of the Privacy Act that strongly indicate individuals would first like to be asked to receive direct marketing from organisations.

Relying upon 'implied consent' as is contemplated by the 'opt out' model in this Proposal fails both 'Privacy by Default' and 'Privacy by Design' principles. Further, implied consent is a legally flawed form of consent which cannot be relied upon as the data controller has pre-determined that they will use the individual's personal information for direct marketing based upon a presumed predisposition to non-objection by the individual. This is the total opposite of consent – choice has been removed and a decision already made for you.

EFA strongly submits that direct marketing only be permitted under the revised Privacy Act subject to the 'fair and reasonable' test coupled with the individual's express consent which is comprised of the following elements:

(a) Voluntary;

(b) Informed;

(c) Current;

(d) Specific, and

(e) Unambiguous indication of the individual's wishes through clear action

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

EFA supports Proposal 20.3 subject also to the presumption an individual must opt in and give their express consent (as defined in our response to Proposal 20.2) to the data controller.

***Proposal** 20.4 Introduce a requirement that an individual's consent must be obtained to trade their personal information.*

EFA supports Proposal 20.4 in principle only. It is internationally recognised both in research and consumer attitudes towards certain classes of data brokers and on-lime advertisers that they are universally not trusted and found not to be worthy of consumer trust.

In particular EFA holds strong objections to those organisations who have historically operated at the margins or outside of privacy laws and are known to have been bad actors by engaging in activities such as hoovering up Commonwealth, State and Territory public records and

repackaging, indexing them in foreign jurisdictions and transferring the data back to Australia to create a detailed profile on Australians. This data is used to create an individual consumer profile and is frequently further augmented and enriched from other third-party data sources. These data sets are then made available for Australian organisations to purchase, rental or use to augment an organisation's own personal information stores.

It is disingenuous at best by some data brokers who claim that the information stored, processed and traded by them is 'de-identified'. Although this might be true in some transactions such as augmenting or appending de-identified data to a third-party customer file, at its heart these organisations exist almost like a secret society in that we, as citizens, have been made members of the secret society, except it is so secret we don't even know we joined and have become members. To describe these data collection activities and uses as nefarious would be exceedingly generous.

EFA submits that data trading be permitted only in circumstances where:

(a) Each proposed data trading activity is subject to an individual's best interest test in addition to the proposed 'fair and reasonableness' test; and

(b) the individual's express consent which is comprised of the following elements:

a. Voluntary;

b. Informed;

c. Current;

d. Specific, and

e. Unambiguous indication of the individual's wishes through clear action.

***Proposal** 20.5 Prohibit direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests.*

EFA strongly opposes Proposal 20.5. EFA submits that direct marketing to a child should be prohibited under the Act, with no exceptions.

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

EFA strongly opposes Proposal 20.6. Targeting children should be a prohibited activity under the revised Privacy Act.

***Proposal** 20.7 Prohibit trading in the personal information of children.*

EFA strongly opposes Proposal 20.7. Targeting children should be a prohibited activity under the revised Privacy Act.

***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.

EFA partially supports Proposal 20.8. In addition to undertaking the 'fair and reasonable' test as contemplated in (a) above, an individual must opt in and give their express consent (as defined in our response to Proposal 20.2) to the data controller to facilitate targeting.

EFA further submits that the Privacy Act should be amended to specifically regulate the use of 'cookies' on line. EFA strongly supports the replication of the legislative approach used to regulate cookies under the General Data Protection Regulation and the ePrivacy Directive as currently enacted in the EU/EEA.

Providing exceptions for socially beneficial content introduces too much risk to an individual's privacy. EFA submits this proposal to be amended to 'targeting individuals based on sensitive information should be prohibited' with no exceptions.

***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.*

EFA supports this Proposal in part but submits that any guidelines should be:

(a) Developed and issued by the OAIC;

(b) Legally binding under the Privacy Act.

21. Security, retention and destruction

***Proposal** 21.1 Amend APP 11.1 to state that 'reasonable steps' include technical and organisational measures.*

EFA supports proposal 21.1.

***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.*

EFA supports Proposal 21.2.

Proposal 21.3 *Enhance the OAIC guidance in relation to APP 11 on what reasonable steps are to secure personal information. The guidance that relates to cyber security could draw on technical advice from the Australian Cyber Security Centre.*

EFA supports Proposal 21.3 in principle and suggests it could be augmented by adopting the approach used under Article 32 of the GDPR, which sets out specific measures to ensure a level of security appropriate to the risk, including, but not limited to:

(a) the anonymization and encryption of personal data

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

(c) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures.

Proposal 21.4 *Amend APP 11.1 so that APP entities must also take reasonable steps to protect de-identified information.*

EFA supports Proposal 21,4 but submits that the OAIC develop guidance on this matter in collaboration with the Australian Cyber Security Centre who can assist with developing technical advice.

Proposal 21.5 *The OAIC guidance in relation to APP 11.2 should be enhanced to provide detailed guidance that more clearly articulates what reasonable steps may be undertaken to destroy or de-identify personal information.*

EFA supports Proposal 21.5 but submits such advice should be developed in collaboration with the Australian Cyber Security Centre.

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.

EFA supports Proposal 21.6 in principle. The retention of personal information is a high risk practice that has real-world consequences for individuals in the case of a data breach. Existing

provisions that require retention of personal information should be reviewed to maximise the privacy of individuals, and minimise the adverse consequence of serious breaches of privacy.

Proposal 21.7 *Amend APP 11 to require APP entities to establish their own maximum and minimum retention periods in relation to the personal information they hold which take into account the type, sensitivity and purpose of that information, as well as the entity's organisational needs and any obligations they may have under other legal frameworks. APP 11 should specify that retention periods should be periodically reviewed. Entities would still need to destroy or de-identify information that they no longer need.*

EFA supports Proposal 21.7 in principle but submits that organisations and agencies develop a systematic Records Management Program under the guidance of an institutional Data Protection Officer/Privacy Officer (as contemplated by Proposal 15.2 and EFA's submission in respect of the same.)

EFA further submits that guidance on the development of a Records Management Program could be developed by the OAIC in consultation with Archives Australia.

Proposal 21.8 *Amend APP 1.4 to stipulate that an APP entity's privacy policy must specify its personal information retention periods.*

EFA supports Proposal 21.8 in principle but questions its effectiveness, given the propensity of individuals to not read Privacy Policies or Collection Statements. Such a proposal creates unnecessary administrative work and pushes the burden of understanding privacy policy onto individuals. Guidance must be given by the OAIC on how best to communicate a records taxonomy/typology and relevant retention periods in these documents.

22. Controllers and processors of personal information

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.

EFA supports this Proposal and further supports the introduction of definitions of data controller, data processor (or data intermediary).

23. Overseas data flows

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.*

EFA supports Proposal 23.1.

***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).*

EFA supports Proposal 23.2 subject to the development of a robust process of consultation inclusive of the publication of Terms of Reference, Discussion Paper and Report. This will ensure that the Government does not inadvertently certify poorly founded and constructed mechanisms such as the APEC Cross Border Privacy Rules Scheme.

***Proposal** 23.3 Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities.*

EFA supports Proposal 23.3 subject to the development of a robust process of consultation inclusive of the publication of Terms of Reference, Discussion Paper and Report.

***Proposal** 23.4 Strengthen the informed consent exception to APP 8.1 by requiring entities to consider the risks of an overseas disclosure and to inform individuals that privacy protections may not apply to their information if they consent to the disclosure.*

EFA strongly opposes Proposal 23.4 as it does not take a Privacy by Default approach and seems to end in a potential result where an Australian citizen loses the protections of the Privacy Act and a data controller is removed of their clear obligation to protect the personal information under their custody or control.

***Proposal** 23.5 Strengthen APP 5 in relation to overseas disclosures by requiring APP entities, when specifying the countries in which recipients are likely to be located if practicable, to also specify the types of personal information that may be disclosed to recipients located overseas.*

EFA supports Proposal 23.5 but submits it should be strengthened by introducing a corresponding requirement to disclose the type of data processing activity being conducted in the relevant foreign jurisdiction.

***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.*

EFA supports Proposal 23.6.

24. CBPR and domestic certification

Nil proposals.

25. Enforcement

***Proposal** 25.1 Create tiers of civil penalty provisions to allow for better targeted regulatory responses:*

(a) Introduce a new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision.

(b) Introduce a new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties.

EFA supports Proposal 25.1 but suggests Part (b) could be enhanced by introducing a new sub-provision that takes account of the practicalities and challenges of compliance that will face small business (assuming the repeal of the small business exception).

***Proposal** 25.2 Amend section 13G of the Act to remove the word 'repeated' and clarify that a 'serious' interference with privacy may include:*

(a) those involving 'sensitive information' or other information of a sensitive nature

(b) those adversely affecting large groups of individuals

(c) those impacting people experiencing vulnerability

(d) repeated breaches

(e) wilful misconduct, and

(f) serious failures to take proper steps to protect personal data.

The OAIC should provide specific further guidance on the factors that they take into account when determining whether to take action under section 13G.

EFA supports Proposal 25.2.

***Proposal** 25.3 Amend the Act to apply the powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 to investigations of civil penalty provisions in addition to the Information Commissioner's current investigation powers.*

EFA supports Proposal 25.3.

***Proposal** 25.4 Amend the Act to provide the Information Commissioner with the power to undertake public inquiries and reviews into specified matters on the approval or direction of the Attorney-General.*

EFA supports Proposal 25.4.

Proposal 25.5 *Amend subparagraph 52(1)(b)(ii) and paragraph 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined:*

> *a declaration that the respondent must perform any reasonable act or course of conduct to <u>identify, mitigate and</u> redress any <u>actual or reasonably foreseeable</u> loss or damage suffered by the complainant/those individuals.*

The OAIC should publish guidance on how entities could achieve this.

EFA supports Proposal 25.5.

Proposal 25.6 *Give the Federal Court and the Federal Circuit and Family Court of Australia the power to make any order it sees fit after a civil penalty provision relating to an interference with privacy has been established.*

EFA supports Proposal 25.6.

Proposal 25.7 *Further work should be done to investigate the effectiveness of an industry funding model for the OAIC.*

EFA strongly opposes this approach. The scheme proposed amounts to a system of indulgences or a license-to-violate-privacy approach. The government is tasked with protecting the privacy of Australians and funds the government through taxes. The lack of funding of the OAIC is a policy choice by the government that can be changed at any time.

Funding the OAIC mostly from high-privacy-risk industries creates an incentive structure that is the polar opposite of what it should be.

EFA strongly disagrees that the model of ASIC represents a success. Australians should not have to pay fees in order to access public information such as company registration details and these fees represent a substantial barrier to transparency, particularly for investigative reporting in the public interest.

The OAIC is a public body established for a public good, not a profit centre. It is not a business and does not need to recoup its costs. The OAIC should be adequately funded within the regular annual budget of the government.

Proposal 25.8 *Further consideration should be given to establishing a contingency litigation fund to fund any costs orders against the OAIC, and an enforcement special account to fund high cost litigation.*

EFA is agnostic on Proposal 25.8. EFA submits that the Government should consider and solve these issues in the same way as it has for the Australian Competition and Consumer Commission which would face the same risks identified here.

Proposal 25.9 *Amend the annual reporting requirements in AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground of section 41.*

EFA supports Proposal 25.9 and further submits as part of its community outreach and education objectives that the OAIC should regularly publish a broad range of complaints and their outcomes in a de-identified manner to assist organisations and agencies meeting their own privacy compliance obligations.

Proposal 25.10 *The OAIC should conduct a strategic internal organisational review with the objective of ensuring the OAIC is structured to have a greater enforcement focus.*

EFA supports Proposal 25.10 and further submits that the OAIC and Information Commissioner's Office be provided with greater funding and resourcing to meet future demands under the revised Privacy Act.

Proposal 25.11 *Amend subsection 41(dc) of the Act so that the Information Commissioner has the discretion not to investigate complaints where a complaint has already been adequately dealt with by an EDR scheme.*

EFA supports Proposal 25.11.

26. A direct right of action

Proposal 26.1 *Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy. The model should incorporate the appropriate design elements discussed in this chapter.*

EFA supports Proposal 26.1. EFA is of the view that the Privacy Act be amended to allow complainants the option of pursuing their matter about a respondent's breach of the APPs (or other types of 'interference with privacy' as defined under the Privacy Act) in a tribunal or court irrespective of whether the matter was dismissed or the subject of an unfavourable decision by the OAIC.

27. Statutory Tort

Proposal 27.1 *Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123.*

Consult with the states and territories on implementation to ensure a consistent national approach.

EFA supports Proposal 27.1 but requests any such consultation process be light touch. There is a good 20 years of research within Australia looking at the creation of a statutory tort for privacy. EFA submits that this is a well canvassed area of privacy law and that the recommendations of the ALRC have been broadly supported for many years.

There is no need to re-investigate this issue in detail once again, and to do so could be interpreted as an attempt to obstruct and delay action on this issue.

28. Notifiable data breaches scheme – impact and effectiveness

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.*

EFA supports Proposal 28.1 in principle.

Proposal 28.2

(a) Amend paragraph 26WK(2)(b) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours.

(b) Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases as soon as practicable.

(c) Require entities to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach.

EFA supports Proposal 28.2 but submits more broadly the Privacy Act be amended in respect of the behaviour of company directors and Responsible Ministers and the oversight of their organisations and agencies compliance with the Privacy Act. There needs to be greater standards of transparency and accountability by organisations and agencies in the context of serious or repeated privacy breaches as this will drive cultural change within those entities and result in better privacy outcomes for Australian citizens.

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.

EFA supports Proposal 28.3 subject to being afforded an opportunity for consultation and comment on the proposed change.

***Proposal** 28.4 Introduce a provision in the Privacy Act to enable the Attorney-General to permit the sharing of information with appropriate entities to reduce the risk of harm in the event of an eligible data breach. The provision would contain safeguards to ensure that only limited information could be made available for designated purposes, and for a time limited duration.*

EFA supports this Proposal in principle only. EFA submits that there should be a risk assessment of such proposed sharing to ensure it does not asymmetrically spread privacy risks or create new privacy risks.

29. Interactions with other schemes

***Proposal** 29.1 The Attorney-General's Department develops a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations.*

EFA supports Proposal 29.1 in principle but strongly submits such a privacy law design guide incorporating Privacy by Default and Privacy by Design principles.

***Proposal** 29.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.*

EFA supports Proposal 29.2.

***Proposal** 29.3 Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.*

EFA supports Proposal 29.3.

30. Further review

***Proposal** 30.1 Conduct a statutory review of any amendments to the Act which implement the proposals in this Report within three years of the date of commencement of those amendments.*

EFA supports Proposal 30.1.

END.