Electronic Frontiers Australia Inc.
ABN: 35 050 159 188
W www.efa.org.au
E email@efa.org.au
@efa_oz

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

10 January 2021

By email

Dear Attorney-General,

RE: Privacy Act Review Discussion Paper

EFA welcomes the opportunity to comment on the Privacy Act Review Discussion Paper.

EFA's 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 communications systems.

Yours sincerely,

Justin Warren
Chair
Electronic Frontiers Australia

Introduction

Holistic view

In the 8 years since reviews closed for the *The Privacy Amendment (Notifiable Data Breaches) Act 2017*, technology has significantly outpaced legislation, and the gap between international legislation and legislation in Australia has widened. Given that many Australian businesses operate globally, this has required enterprises to be informed of many disparate rules and regulations. Bringing the Australian Privacy Act in line with international legislation - e.g. GDPR, CCPA - would produce efficiency gains for Australian businesses, as they would no longer be managing multiple and often conflicting data handling requirements.

EFA recommends that after reviewing the feedback to the proposals individually, and incorporating such changes as are deemed appropriate, that the interaction of the various components should then also be reviewed *as a whole*. As discussed in our submissions, and those of many others, the interactions between the different parts of the Privacy Act with each other, and with other legislation, can lead to perverse outcomes.

The intended impact of a renewed Privacy Act should be carefully reviewed against likely attempts to deliberately bypass or undermine its restrictions and protections. Good intent should not be assumed, and the incentive structures created by the Privacy Act should be assessed with a sceptical eye. EFA also counsels mindfulness of the possibility for inadvertent harms without malicious intent or foreknowledge, in response to which defaults that prioritise privacy must serve as safeguards against unintended consequences and function creep.

We encourage the view of privacy as a collective good, not just an individual benefit. Some acts and practices are harmful to privacy society-wide, even though they may provide some benefits to a privileged subset of the population. Sometimes the needs of the many should outweigh the desires of the few.

Summary of Recommendations

1. Include a list of factors that must not be taken into account when balancing the public interest against other interests.
2. Explicitly include consideration of societal harms from loss of privacy in Proposal 10.2.
3. Include additional clarification of the intended meaning of ‘relates to’ in the definition of ‘personal information’.
4. Delete the word ‘reasonably’ from Proposal 2.3.
5. Explicitly include individuation, as well as identification, of individuals in the definition of personal information.
6. The definition of personal information should include information or opinion provided, collected, created, generated or inferred.
7. Abandon the Privacy Amendment (Re-identification) Offence Bill 2016 completely.

8. Abolish the current exemptions for small businesses, employee records, and political acts and practices.
9. The small business exemption should be abolished.
10. The employee records exemption should be abolished.
11. The political acts and practices exemption should be abolished.
12. The journalism exemption should be abolished and replaced with a more limited exemption for investigative and public interest journalism.
13. That the collection, use, and disclosure of personal information for investigative and public interest journalism be subject to a mandatory industry Code approved and regulated by the Privacy Commissioner.
14. Amend the definition of 'consent' in Proposal 9.1 to explicitly require consent that has not been subsequently withdrawn.
15. The Privacy Act should mandate a fairness framework that applies to all uses of personal information by all entities and that cannot be bypassed by any other law.
16. When balancing harms against benefits, evidence of claimed harms or benefits should be required, proportional to the magnitude of the claim.
17. Introduce pro-privacy settings enabled by default.
18. The ability to withdraw consent should form part of the definition of valid consent.
19. That the collection, use, and disclosure of information about or relating to Australian children should prioritise the best interests of the child, taking into account a graduated approach to children's autonomy and decision-making ability.
20. Legislation should not require age verification technologies to protect privacy.
21. Include a right to human review of any automated decision-making system that uses personal information.
22. Require any automated decision-making system that uses personal information to be transparent, explainable, and auditable.
23. Consent should be required before using data for any secondary purpose not directly related to or reasonably necessary to support the primary purpose.
24. Include definitions of both 'use' and 'disclosure' in the Privacy Act that are consistent with the current definitions in the APP Guidelines.
25. Fund the OAIC directly as part of the regular government budget.

Part 1: Scope and application of the Act

Objects of the Act

We support the addition of a public interest test.

Proposal 10.1 is highlighted as inter-operating with the objects to require a balancing of competing interests.

We support Proposal 10.2 as a set of legislated factors that must be taken into account when balancing competing interests. We recommend that there should also be a list of factors that must *not* be taken into account. This approach would mirror the mechanisms present in the *FOI Act*[1].

Recommendation: Include a list of factors that must *not* be taken into account when balancing the public interest against other interests.

We also recommend that the list of factors in Proposal 10.2 explicitly includes consideration of societal harms, not merely the risks or impacts on particular individuals, in order to recognise privacy as a collective concern within the legislation itself. This would make clear that, in weighing up competing interests, the interests of society more generally must also be taken into account, not merely the competing interests of individuals.

Recommendation: Explicitly include consideration of societal harms from loss of privacy in Proposal 10.2.

Definition of 'personal information'

We are encouraged that many of the recommendations made in our submission to the Issues Paper have been adopted by Proposals 2.1-2.5. We recommend further refinements to the proposals to ensure they are made fit-for-purpose.

We support the intention of Proposal 2.1 to change the word 'about' to 'relates to' as this would bring the Privacy Act into greater alignment with other legislation, including the GDPR and other international privacy laws.

However, we recommend that additional clarity is provided in order to avoid a repeat of the *Telstra Corporation Limited and Privacy Commissioner*[2] (Telstra) decision. It should be made clear that 'relates to' means:

- the individual is a subject of the information, or
- if the information concerns or links to the individual, or

[1] See, e.g. *Freedom of Information Act 1982* (Commonwealth Consolidated Acts) 11B ('*FOI Act*').
[2] *Telstra Corporation Limited and Privacy Commissioner* [2015] Administrative Appeals Tribunal of Australia 991.

- if the intent or effect of dealing with the information is to learn, evaluate, make a decision about, influence the status or behaviour of, treat in a particular way, or otherwise have an impact upon the individual.

Recommendation: Include additional clarification of the intended meaning of 'relates to' in the definition of 'personal information'.

Delete 'reasonably'

We strongly recommend removing the word 'reasonably' from Proposal 2.3. Either an individual is identifiable, or they are not.

Legislation in a variety of international jurisdictions[3] provides for an identifiability threshold without a 'reasonable' qualifier. It is a substantial weakness to the *Privacy Act* and should be removed.

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.

Systemic privacy harms can result from a single 'unreasonable' application of resources to identify individuals in a dataset. Often the method used to attempt to de-identify any one individual has been used for all individuals in a dataset, and thus discovering a weakness that allows for the identification of one individual effectively unmasks them all.

Recommendation: Delete the word 'reasonably' from Proposal 2.3.

Individuation as well as identification

Privacy harms can result from the singling out of individuals, even if their specific *identity* is not known. As noted in the Privacy Act Review Discussion Paper, it is possible to single out an individual using data profiling with the combination of very few data points; "the Ad tech Inquiry interim report cited findings that between 61 and 87 percent of individuals in the United States were able to be identified by a combination of ZIP code, birth date and gender"[4]. This *singling out* must therefore also be explicitly covered by the definition of personal privacy, lest organisations that engage in intrusive surveillance attempt to bypass the Privacy Act by arguing that they do not identify people.

---

[3] Including the GDPR, the national privacy laws of New Zealand, Canada, Singapore, South Africa, Brazil, Nigeria, Japan, Hong Kong, India, and the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

[4] ACCC, Digital Platforms Inquiry report (n 2) 49. <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>

The issue of individuation is explored in great detail by Salinger Privacy in their submission to this review[5] and we commend it to you.

Recommendation: Explicitly include individuation, as well as identification, of individuals in the definition of personal information.

Include inferred or generated data as 'personal information'

Information or data that is generated or inferred about individuals should be included in the definition of personal information. It is incorrect[6] to claim that there is no privacy harm that can result from actions that refer to, result from, or expose information about people that is inferred or generated.

There is an easily apprehended harm in correct inferences being drawn and then exposed to third parties without consent; a well-popularised example from as long ago as 2012 featured a teenage girl's pregnancy inferred from her grocery purchases by a loyalty program and then revealed to her father via advertising without her consent or knowledge.[7] There is also harm in *incorrect* inferences being drawn and exposed — say, a woman buys groceries for a pregnant friend and then her abusive spouse concludes she's unfaithful. Pregnancy status is intimate, personal health information; whether or not a person is pregnant is extremely private, and until and unless they decide to share that information with anyone else it should remain so. Significantly, a person should have agency about the discovery of private information about themselves, not have it thrust upon them by commercial interests.

Recommendation: The definition of personal information should include information or opinion provided, collected, created, generated or inferred.

Abandon the Re-identification Offence Bill

We strongly oppose Proposal 2.6 to re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016. This Bill was a knee-jerk reaction by an embarrassed government that sought to penalise independent researchers for discovering significant flaws in government data handling practices.[8]

The Bill was much criticised at the time, including by the Privacy Commissioner, and we do not believe it is capable of being salvaged. Its entire approach is based on a fatally flawed view of modern information security practices and it is astonishing (and somewhat embarrassing in and

---

[5] Anna Johnston, 'Submission in Response to the Privacy Act Review – Discussion Paper , October 2021' (Salinger Privacy, 3 January 2022) <https://www.salingerprivacy.com.au/wp-content/uploads/2022/01/22-01-03_Privacy-Act-review_Salinger-Privacy_Submission.pdf>.

[6] EFA would go so far as to say it is naïve and dangerous if not outright mendacious.

[7] Charles Duhigg, 'How Companies Learn Your Secrets', *The New York Times* (online, 16 February 2012) <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.

[8] Stephanie Anderson, 'Medicare Data Pulled over Breach Concerns', *ABC News* (Text, 29 September 2016) <https://www.abc.net.au/news/2016-09-29/medicare-pbs-dataset-pulled-over-encryption-concerns/7888686>.

of itself) that re-introducing the Bill was even considered, let alone proposed. The Bill should be abandoned.

The issue of malicious re-identification can be better regulated in other ways, such as a statutory tort as outlined in Proposal 26.

Recommendation: Abandon the Privacy Amendment (Re-identification) Offence Bill 2016 completely.

Exemptions from the Privacy Act

EFA submits that the Privacy Act should cover equally all entities dealing in the personal information of Australians. We therefore recommend that the current exemptions for small businesses, employee records, and political acts and practices should be abolished.

All organisations should have the same obligations, and all individuals the same rights, when it comes to the appropriate handling of personal information.[9]

Recommendation: Abolish the current exemptions for small businesses, employee records, and political acts and practices.

Small business exemption

The harms to privacy are the same whether they were caused by failures at a small or large organisation, in a similar way that harms to health are the same if a person is poisoned by a coffee from a local cafe or coffee from a multi-national chain. We expect certain minimum standards for safe food handling practices and we should have the same expectations for safe handling of our personal information.

The nature of digital information in particular means that a small business can hold a very large amount of personal information about a very large number of individuals. Indeed, not being covered by the Privacy Act creates an incentive for large, potentially better resourced organisations to avoid collecting such large datasets while small, poorly resources businesses have a perverse incentive to collect personal information as they are free of the obligations of the Privacy Act to keep it safe.

We do not follow the logic that unsafe privacy practices should be permitted simply because the organisation doing it is small. The flexible nature of the APPs can already cope with the differing circumstances of differently sized businesses, such as with the existing Data Security obligations.

Recommendation: The small business exemption should be abolished.

[9] Anna Johnston (n 5) 17.

Employee records exemption

All organisations should have the same obligations, and all individuals the same rights, when it comes to the appropriate handling of personal information.

We see no logical justification for the existence of the employee records exemption and recommend that it be abolished.

Recommendation: The employee records exemption should be abolished.

Political acts and practices exemption

We see no logical justification for the existence of the political acts and practices exemption and recommend that it be abolished.

The abuse of personal information to annoy voters is extremely unpopular and reduces public confidence Australia's political process.[10] Failure to abolish this exemption would appear extremely self-serving by Parliament, and is contrary to the wishes of the vast majority of Australians.[11]

Recommendation: The political acts and practices exemption should be abolished.

Journalism exemption

We submit that the broad journalism exemption should be abolished and replaced with a very limited exemption to collect, use, and disclose (as per APPs 3, 5, and 6) information only where it is necessary for the conduct of investigative and public interest journalism.

Recommendation: The journalism exemption should be abolished and replaced with a more limited exemption for investigative and public interest journalism.

We further recommend that the collection, use, and disclosure of personal information for investigative and public interest journalism should be subject to a mandatory industry Code approved and regulated by the Privacy Commissioner, with appropriate appeal rights.

Recommendation: That the collection, use, and disclosure of personal information for investigative and public interest journalism be subject to a mandatory industry Code approved and regulated by the Privacy Commissioner.

---

[10] 'Craig Kelly Texts Show Need for Spam, Privacy Reform: Experts', *InnovationAus* (1 September 2021) <https://www.innovationaus.com/craig-kelly-texts-show-need-for-spam-privacy-reform-experts/> ('Craig Kelly Texts Show Need for Spam, Privacy Reform').

[11] David Crowe, 'Voters Want to Ban Politicians from Spamming Them with Texts and Calls', *The Sydney Morning Herald* (25 September 2021) <https://www.smh.com.au/politics/federal/voters-want-to-ban-politicians-from-spamming-them-with-texts-and-calls-20210924-p58uko.html>.

Part 2: Protections

Notice and consent

EFA supports proposals 8.1-8.4 and 9.1-9.2. We also reiterate our earlier comments on the Issues Paper regarding a notice and consent approach to privacy protection.

We suggest that the idea of 'current' consent in Proposal 9.1 should be explicitly and clearly drafted such that consent is only valid if it is consent *that has not been subsequently withdrawn*. Such consent would no longer be current.

EFA is concerned that those who have currently enjoyed a long period of somewhat lax, flexible, and frequently self-serving definitions of 'consent' will enthusiastically attempt to find creative new ways to define consent in perverse but ultimately self-serving terms. Indeed, many entities have substantial financial incentives to do so. Such attempts should be vigorously opposed from the outset or we risk Australians needing to spend further years arguing in various venues, at great personal cost, about the precise definition of 'voluntary', 'specific', etc.

Recommendation: Amend the definition of 'consent' in Proposal 9.1 to explicitly require consent that has not been subsequently withdrawn.

Fair and reasonable

Australians should be able to rely on a fundamental level of privacy protection that does not require constant, active vigilance on their part.

There are acts and practices that are so harmful to privacy, either individually or collectively, that any purported 'consent' cannot be deemed valid. The concept of unfair contract terms is a well recognised area of contract law[12] and Proposals 10.1-10.2 do much to assist in encoding this principle into the Privacy Act.

However, the protections of the Privacy Act should not be able to be undermined by other laws, particularly where consent is not required or allowed for. A great deal of personal information is collected, used, or disclosed by government agencies by compulsion, coercion, not with consent, and the *fair and reasonable* test should apply in *all* circumstances, including these.

Further, there should be legislated guidance as on acts and practices that would meet the fair and reasonable rest, and those that would not.

Recommendation: The Privacy Act should mandate a fairness framework that applies to all uses of personal information by all entities and that cannot be bypassed by any other law.

---

[12] Australian Competition and Consumer Commission, 'Unfair Contract Terms', *Australian Competition and Consumer Commission* (Text, 15 September 2015) <https://www.accc.gov.au/business/business-rights-protections/unfair-contract-terms>.

Harms proportional to benefits

EFA suggests that the generic 'fair and reasonable' test should be enhanced with a legislated balancing of harms against benefits. This is particularly relevant for cohorts of people, such as children, at increased risk of harm from generic services.

Some care will need to be taken with subjective versus objective weighting of harms compared to benefits. What may be harmful to a particular individual or group may not be harmful to a different individual or group; their individual or group circumstances should be taken into account. For example, a person fleeing an abusive partner may be at increased risk of harm from unauthorised disclosure of their location, but still want to be able to exercise with close friends at a nearby park. They are at much greater risk of harm from having their location inadvertently disclosed by an exercise app than a group of runners competing in a public race; default privacy settings should do the least harm.

Conversely, systemic practices are more appropriately judged against more objective measures or documented community standards, rather than those particular to specific individuals or groups.

In all cases, it should be clear from the outset how a given system can meet the *fair and reasonable* threshold before it is implemented. This will go some way to avoid disingenuous claims that harmful effects could not have been predicted and are therefore somehow less harmful than if they had been predicted and remediated. Likely privacy-related harms are frequently obvious to those with relevant expertise, yet ignorance is often claimed by decision makers after the fact as protection from accountability for adverse outcomes experienced by victims. A *fair and reasonable* threshold would help to assure that appropriate risk assessments form part of the due diligence process of system design, and their absence would indicate a failure to appropriately engage with the Privacy Act.

EFA also recommends favouring evidence of *actual* harms and *actual* benefits over purported intents or claimed benefits. Nebulous claims of outsize future benefits are frequently used to justify collection or use of personal information without informed consent (but what if it cures cancer!) yet the alleged future benefits then fail to materialise. This *big data exceptionalism* approach to personal information should be actively discouraged. Extraordinary claims require extraordinary evidence.

Recommendation: When balancing harms against benefits, evidence of claimed harms or benefits should be required, proportional to the magnitude of the claim.

Pro-privacy defaults

Australians should be able to rely on a fundamental level of privacy protection that does not require constant, active vigilance on their part.

We should be able to assume that our privacy is protected to a minimum standard without active intervention or privileged access to material resources and cultural capital on our part. Clear,

preferably objective, standards reflecting community expectations should protect the privacy of Australians by default, as Australian Consumer Law[13] provides fundamental protections for consumers that cannot be contracted away.

A common standard that applies to all entities would be easier for Australians to understand, and easier for entities to comply with. EFA believes that Proposal 12 Option 1 will help to normalise the expectation that privacy should be protected by default.

EFA does not support Option 2 as sufficient to provide adequate privacy protections, particularly to those with lower digital literacy. Lower digital literacy predisposes for a higher risk of privacy harms, and the onus should not be on those at greater risk to take extraordinary protective measures —which they may not even be aware of, let alone understand—in order to have their privacy protected.

Indeed, it is unclear how "default to less privacy" could constitute valid consent under the proposed changes to the definition of consent that have been proposed. Failing to "Click here for more privacy" is not the same as actively choosing to disable privacy settings in order to share content or make your profile visible to others. Option 1 is the only option that would be compatible with the proposed (and EFA's preferred) definition of consent.

Recommendation: Introduce pro-privacy settings enabled by default.

Right to object

EFA submits that if consent cannot be withdrawn then it cannot be said to be freely given in the first place, and so Proposal 14 is somewhat redundant. We also submit that the phrasing of 'right to object' is unhelpful as an objection may be made but not honoured, particularly in cases where consent was not sought in the first place, such as when collection of personal information is compelled by agencies including the ATO, Centrelink, and the Department of Health.

We question the utility of objecting to the collection of information where there is no intention of seeking consent in the first place.

Recommendation: The ability to withdraw consent should form part of the definition of valid consent.

Children and privacy

EFA supports the proposal to include an assessment of whether an activity is in the best interests of a child as a factor of the 'fair and reasonable' test (Proposal 10.2). EFA asks why this test should not apply to the collection, use, or disclosure of the personal information of an adult as well?

Far too much invasive surveillance of Australians of all ages by over-enthusiastic engineers,

[13] *Competition and Consumer Act 2010.*

marketers, and educators happens merely because it is possible, not because it is useful or right. Amending the Privacy Act to cover this kind of information is long overdue, and has long been demanded by the vast majority of the Australian populace.[14]

Of the options proposed in Proposal 13, EFA supports Option 2 and does not support Option 1.

EFA believes that childrens' autonomy should be respected, and notes that parents and guardians sometimes, sadly, do not act in their own childrens' best interests. This can be particularly challenging in situations where multiple adults have responsibility for a child but do not agree on the best course of action. Legislation that specifically denies a child's autonomy in such cases would be deeply unfair, particularly when age-limits provide arbitrary lines that do not take into account the particular child's decision-making ability.

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* would be inappropriate, as the Discussion Paper notes.

EFA strongly supports the concept of *assumed age of capacity* as noted in Proposal 13.1 as a mechanism to provide for childrens' autonomy within a supportive framework that takes into account the differing needs of children at different stages of development.

Recommendation: That the collection, use, and disclosure of information about or relating to Australian children should prioritise the best interests of the child, taking into account a graduated approach to children's autonomy and decision-making ability.

Age verification

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. In order to determine if an individual is a child, the person must be individuated (violating the goal of not singling out individuals without their consent discussed above) and their age must be assessed, which requires additional information that may not have otherwise been necessary to collect or use. Ironically, society-wide harms to privacy predictably result from some efforts to protect children's privacy, such as any requirement that all adults prove they are adults before they can access communication services. EFA does not support such efforts.

Some parties like to rhetorically claim that the online world should be governed by the same laws that apply offline, and we note that the vast majority of activities undertaken by people in the physical world do not require age verification. Why, then, should we need to prove we are adults in order to participate in society online?

---

[14] 'Australian Community Attitudes to Privacy Survey 2020', *OAIC* <https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/>.

The challenges of privacy online are a result of a *distinct lack* of legislated privacy defaults, despite years of demands for better privacy protections.[15] This has lead to widespread surveillance online *because it is easy and/or possible* in ways that are not offline. A handy solution presents itself: stop it.

There is no fundamental reason why online surveillance has to exist. EFA strongly believes that it does not. Rather than attempting to find complex, technological workarounds to problems that shouldn't exist, we say there is a far simpler and more straightforward approach: stop spying on people.

Recommendation: Legislation should not require age verification technologies to protect privacy.

Automated decision-making

EFA does not support Proposal 17 because we believe it will have no effect.

Instead, the Privacy Act should include a right to human review of any automated decision, and a requirement that any automated decision-making system should be transparent, explainable, and auditable.

The use of personal information to make automated decisions should be subject to the same 'fair and reasonable' test as all other uses of personal information, as discussed above.

Recommendation: Include a right to human review of any automated decision-making system that uses personal information.

Recommendation: Require any automated decision-making system that uses personal information to be transparent, explainable, and auditable.

Research exemptions

The Discussion Paper asks if the proposed definition of *secondary purpose* will inadvertently restrict socially beneficial uses and disclosures or personal information such as public interest research. EFA does not believe this will be a substantial problem and can readily be addressed by seeking consent.

EFA is concerned that overbroad claims of the alleged benefits of research are used to justify invasive surveillance practices, and to bypass the need for consent. Large datasets have been accumulated under lax privacy protections to date, and the fact that this was possible does not mean it *should* have occurred. It is inappropriate to take a proprietary approach to these datasets and assume that—since they exist—they should therefore be used in research because there may be some nebulous future benefit.

---

[15] 'Australian Community Attitudes to Privacy Survey 2017', *OAIC* <https://www.oaic.gov.au/updates/videos/australian-community-attitudes-to-privacy-survey-2017/>; 'Australian Community Attitudes to Privacy Survey 2020' (n 7).

While EFA is supportive of evidence-based decision making, *big data exceptionalism*[16] should not be sufficient justification for privacy-invasive data collection, use, and disclosure. A great deal of information is collected by governments through compulsion, coercion, and under threat of force; consent is not an option. Why should this data be made available to researchers simply because it exists and they think it might be useful? Why is seeking consent for its secondary use not an option?

EFA is aware that seeking consent can be costly and time-consuming, but we question whether saving money is sufficient justification for the violation of people's privacy and to override lack of consent. It is possible that some research outcomes may justify it, but we submit that they are few and far between. An alternative is that research funding should be increased in order to support more ethical data collection methods. Why should money have more rights than people?

Recommendation: Consent should be required before using data for any secondary purpose not directly related to or reasonably necessary to support the primary purpose.

Overseas data flows

EFA reiterates our submission to the Issues Paper that overseas data flows could be addressed by transparency, privacy by design, and free, full and informed consent to the overseas sharing of data.

Prescribed countries and schemes

EFA supports Proposal 22.1 to provide a mechanism that will prescribe countries and certification schemes under APP 8.2(a). This will provide greater clarity to Australians on which countries and schemes provide similar or better privacy protections to Australia's privacy laws.

Strengthen notice requirements

EFA supports Proposal 22.4 to include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas in an entity's up-to-date APP privacy policy.

When combined with Proposal 22.1, this should provide sufficient information for Australians to accurately assess whether or not their personal information will enjoy the same protections as in Australia when disclosed overseas.

Define 'disclosure'

EFA supports including definitions of *use* and *disclosure* in the Privacy Act. Increased clarity of the meaning and intended outcome of laws can only be a good thing.

---

[16] Helen Nissenbaum, *Deregulating Collection: Must Privacy Give Way to Use Regulation?* (SSRN Scholarly Paper No ID 3092282, Social Science Research Network, 1 May 2017) <https://papers.ssrn.com/abstract=3092282> ('*Deregulating Collection*').

Recommendation: Include definitions of both 'use' and 'disclosure' in the Privacy Act that are consistent with the current definitions in the APP Guidelines.

Clarify 'reasonable steps'

EFA supports Proposal 22.6 to improve the clarity of what *reasonable steps* means by amending the Privacy Act. EFA suggests that the clarifications should make such steps explicit and, as far as possible, objectively assessable.

GDPR adequacy

EFA strongly supports moves to improve Australia's privacy laws to achieve a GDPR adequacy determination. Such moves would do much to improve the privacy of Australians, reduce the regulatory burden on Australian businesses, and enhance Australia's ability to participate in the global information environment. These moves are long overdue.

Right to erasure of personal information

While the measures contained in Proposal 15 are encouraging, EFA believes they do not go far enough.

We submit that the "right to erasure" as expressed at Art. 17 of the GDPR ought to be introduced into Australian law. Personal information ought not be retained for any period longer than is reasonably necessary to achieve the purpose of the collection, and security favours a default that data is not retained longer than reasonably necessary.

We respectfully submit that personal information ought to be deleted on the earlier of the completion or cessation of the reason for which it was collected or twelve months (12) unless the data subject has provided full, free and informed consent that the data be stored for a longer duration that does not exceed seven (7) years.

EFA does not support a blanket exemption of unreasonableness as contained in Proposal 15.3. If the cost of complying with a data erasure request from an individual is too great, then the Act should be designed to encourage organisations to take a minimisation approach to data handling and not collect data from individuals that it does not have the capacity to appropriately handle.

There should be very few reasons data erasure is not possible, and these should be clearly noted before the information is collected. Otherwise, consent cannot be withdrawn and therefore cannot be validly given as discussed above. If entities determine that erasure (in order to comply with the removal of consent) is not possible after data collection has occurred, they risk placing themselves in a *Catch-22* situation where they cannot comply with the Privacy Act with regard to consent and also cannot bring themselves into compliance with the Privacy Act.

Part 3: Regulation and Enforcement

Incentive structures

EFA suggests that any changes to regulation and enforcement must take into account the incentive structures created by the resulting framework. Currently there are few incentives to employ privacy-by-default design practices, and entities that do tend to be at a competitive disadvantage relative to those that do not.

Any penalties for poor behaviour tend to be much delayed, long after the benefits of privacy violations have accrued to the badly behaving entities. Often these entities continue to enjoy derivative benefits obtained in this fashion even if an adverse determination is eventually made against them. For example, while Clearview.AI was instructed to destroy certain information collected about Australians[17], it was not instructed to destroy all information *derived* from the unlawfully collected information, which could be considered the proceeds of a crime.

This creates a strong incentive for bad actors to move quickly to perform as many unlawful or unethical privacy violations as possible before they are (sometimes) caught and (perhaps) punished. If an entity manages to gain sufficient size before it is caught, these practices are simply good business as it is able to absorb any small financial penalty or minor reputational damage and then carry on as before, discarding the personal information it no longer needs as it has already extracted all of the value from it.

EFA suggests that the Privacy Act should describe a system with *inherent* incentives that encourage good privacy practices and discourage bad ones such that the system generally tends towards a state of self-regulation and privacy enhancement.

EFA humbly suggests that the existing system has manifestly failed to achieve this goal, and doing more of the same is unlikely to improve matters.

The OAIC

Proposals 24.1-24.5 seek to add additional powers and abilities to the OAIC. While EFA believes these proposals may well help, the primary issue with the OAIC is lack of funding.

EFA submits that OAIC is an ineffective regulator due to its deliberate under-funding over many years combined with systematic attempts to undermine its function. Adding additional powers and responsibilities will make this problem worse, not better.

Laws that are not enforced effectively do not exist, and the OAIC is unable to enforce privacy laws in a comprehensive and timely fashion. Due to lack of resourcing, the OAIC is forced to choose only relatively high-impact or systemic privacy issues to focus on, and any action taken

[17] *Commissioner initiated investigation into Clearview AI, Inc (Privacy)* [2021] Australian Information Commissioner 54.

is slow. This leaves many individuals and groups with no recourse to privacy harms they may suffer, and systemic harms to groups persist while the OAIC gradually makes its way through an investigation.

"The same OAIC, only more so" is unlikely to achieve an improved regulatory result.

Industry levy

EFA strongly opposes Proposal 24.7 for an industry levy to fund the OAIC.

The scheme proposed amounts to a system of indulgences[18] 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 industry 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[19], and these fees represent a substantial barrier to transparency, particularly for investigative reporting in the public interest.

The OAIC is 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.

Recommendation: Fund the OAIC directly as part of the regular government budget.

Splitting out functions

EFA does not support Proposal 24.9.

The issue described arises due to the lack of funding for the OAIC and the solution is to provide it with increased funding by direct budget allocation. The options proposed will simply continue the systematic undermining of the OAIC that will render the majority of the proposals in the Discussion Paper moot.

Direct right of action

EFA submits that a direct right of action should be framed as an alternate option to action by the OAIC (or other regulatory bodies) that acts as a check on the success or failure of regulators. Recent Royal Commissions have highlighted that, on occasion, regulators have been unable to

[18] *Wikipedia* (online at 10 January 2022) 'Indulgence'.
[19] Particularly given that annual company registration fees have already been paid by the companies themselves.

adequately protect individuals and that an alternate pathway is sometimes required to ensure justice.

EFA submits that successful action by the government in protecting privacy would alleviate the need to make use of a direct right of action. A direct right of action would thus act as a useful indicator of how well privacy protections are working and would highlight areas that may need further adjustment.

EFA also supports the recommendations made by Salinger Privacy regarding direct right of action from page 44 of their submission, particularly in regards to providing an accessible and no-cost tribunal with a cap on damages.

Statutory tort

EFA continues to be a supporter of a statutory tort for serious invasion of privacy as recommended by the Australian Law Reform Commission, i.e. Option 1 as provided by the Review[20].

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.

[20] 'A Statutory Cause of Action for Serious Invasion of Privacy', *ALRC* <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-dp-80/4-a-new-tort-in-a-new-commonwealth-act/summary-138/>.