Submission by Free TV Australia

Privacy Act Review

December 2020

Table of contents

1. Executive Summary

- This review of the Privacy Act has arisen out of the findings of the ACCC's Digital Platforms Inquiry Final Report (DPI Report). It found that, while digital platforms provide a wide range of valuable services to consumers in exchange for data, because of the volume and scope of data being collected by these platforms in respect of many different aspects of consumers' personal lives, the nature of that exchange is often unclear to consumers. This is resulting in:
    - Lack of knowledge or awareness of the data practices of digital platforms by consumers (a lack of transparency); and
    - Consequently, consumers not being able to make informed choices about how to engage with these platforms in a manner that aligns with their privacy preferences (a lack of control).
- In Free TV's view, the Privacy Act provides a strong foundation to deal with these issues – it already unequivocally requires organisations to be transparent about the data they collect, how they collect it, and the purposes for which they use it.
- The Privacy Act was deliberately drafted to be a principles-based and technology neutral part of a three-tiered regulatory framework comprising:
    - High-level principles of general application in the Act
    - Regulations and industry codes detailing the handling of personal information in specific contexts, and
    - Guidance issued by the Privacy Commissioner dealing with operational matters and explaining to end users what is expected in various circumstances as well as advice and education.
- This approach remains the most appropriate approach to adopt. However, the ACCC's findings highlight issues with effective implementation of the provisions of the Act and how they are being interpreted in very specific circumstances – that is, with the tiers of the framework intended to support the legislation, rather than the legislation itself).
- For this reason, Free TV's view is that the most effective way to address the issues identified by the ACCC is to:
    - strengthen the regulatory support structures underpinning the Privacy Act including through better research of data practices, guidance on interpretation of the principles including how the law applies to these practices in specific circumstances, and
    - Ensure the OAIC is sufficiently resourced to effectively enforce the law so that organisations are incentivised to ensure their data practices comply, rather than addressing issues once large-scale privacy breaches have occurred.
- In accordance with this approach to reform, in relation to the specific provisions of the Privacy Act, Free TV:
    - Strongly opposes any proposed amendments to the Act to deem IP addresses, device identifiers, location data and other online identifiers to be 'personal information' in the absence of being combined with other information from which an actual person can be identified.
    - Does not support strengthening the existing consumer consent obligations in the Act – these are already comprehensive. Any amendments which would unnecessarily slow

down consumers' online experiences or increase the problem of "consent fatigue" are strongly opposed.

- Strongly supports the retention of the journalism exemption. This exemption appropriately balances the competing interests of freedom of speech and the free flow of information with the privacy rights of individuals and is critical to a healthy democracy.
- Strongly opposes introduction of a statutory tort for invasion of privacy. This would fail to address the issues identified by the ACCC, is not necessary and would place undue weight on an individual's right to privacy at the expense of freedom of communication.
- Does not support amending the Privacy Act to give individuals a direct right to bring actions and class actions against APP entities.

2. Introduction

Free TV Australia is the peak industry body for Australia's commercial free-to-air broadcasters. We advance the interests of our members in national policy debates, position the industry for the future in technology and innovation and highlight the important contribution commercial free-to-air television makes to Australia's culture and economy.

Free TV proudly represents all of Australia's commercial free-to-air television broadcasters in metropolitan, regional and remote licence areas.

We welcome this opportunity to submit our views to the Privacy Act Review Issues Paper (Issues Paper).

As indicated in the Issues Paper, this review has arisen in response to the ACCC's Digital Platforms Inquiry, following which the Government committed to undertake a review of the Privacy Act and to consult on options to better empower consumers to protect their data in the digital economy.

Free TV agrees that the Privacy Act should empower consumers, protect their data as well as serve the Australian economy. However, it should also be able to adapt to changing technologies and evolving practices in relation to consumer data over time.

Our current privacy regulations were developed with the intention that they form part of a tiered framework which sets out broad flexible and adaptable principles in legislation, but is supported by guidance documents, research and monitoring and enforcement.

In this submission we set out:

- Part A – the preferred approach to reform in the context of the issues raised by the ACCC's Digital Platforms inquiry as well as the structure of our existing framework.

- Part B – our comments on the specific areas for reform being considered in this inquiry.

In summary, while we are not convinced that an overhaul of the existing principles-based approach to the Act is necessary, there is no doubt that a contemporary approach to regulation is required so that digital platforms are effectively incentivised to be transparent in relation to their data practices. Such an approach requires effective guidance, ongoing monitoring and research in relation to evolving technologies and data practices, education of consumers, and enforcement, as was envisaged in the drafting of the Act.

3. PART A – APPROACH TO REFORM

In this section we:

- Examine the key issues identified by the ACCC
- Set out how the existing regulatory framework deals with these issues; and
- Propose an approach for reform.

3.1 The findings of the ACCC

Before considering fundamental changes to the existing laws, it is first necessary to consider the problems identified by the ACCC, and whether the existing Act or other aspects of the regulatory framework are deficient.

This review has arisen out of the ACCC's Digital Platforms Inquiry Final Report (DPI Report). The DPI report found that digital platforms provide a wide range of valuable services to consumers in exchange for data. While this is not problematic per se, the key issue identified by the ACCC was that the nature of this exchange is not always clear to consumers. In particular:

- Digital platforms can collect a wide range of beyond what the user actively provides and of which they may be unaware.
- Consumers' current relationship with digital platforms prevents them from making informed choices due to bargaining power imbalances
- Information asymmetries make it difficult for consumers to assess the current and future costs of handing over their data
- Privacy policies and consent processes on digital platforms often contribute to these problems because they do not give consumers the information they need in a meaningful or effective way.[1]

It found that this was a particular problem on digital platforms due to the volume and scope of data being collected by these platforms in respect of many different aspects of consumers' personal lives. It identified three practices by digital platforms in particular as problematic and in relation to which consumers expressed concern:

- the collection of location data – particularly not knowing how that data was being used or shared with third parties
- online tracking of consumers for targeted advertising purposes, particularly due to the fact that it is unclear exactly what is being tracked and who it is being shared with, and particularly in circumstances they would not expect, for example when they are not logged into their account, and
- the sharing of user data with unknown third parties.[2]

In relation to these areas of particular concern, it identified the crux of the issue to be

a) the consumers lack of knowledge or awareness of the data practices of the digital platforms (lack of transparency); and

[1] Digital Platforms Inquiry Final Report, Chapter 7, p 374.
[2] Ibid.

b) that this lack of awareness was leading to consumers not being able to assess or make informed choices about how to engage with these platforms and that align with their privacy and data collection preferences (lack of control). [3]

Free TV agrees with the ACCC's findings that transparency and control are key to a functioning privacy framework. They are essential to the validity of a consumer's consent to use of their personal information.

3.2 Approach to regulation under the existing framework

Concepts of transparency and control are not new and are in fact directly dealt with under the existing Act. The purpose of the privacy regulatory framework has always been to give consumers control over their personal information and to give them tools to choose what they want to share and the circumstances in which they want to share it. In this way privacy is aimed at facilitating people's engagement with the world around them, by balancing privacy interests with practical concerns.

These concepts of transparency and control are dealt with under the existing framework through the Privacy Principles. While broadly stated, they clearly require organisations to be transparent about the data they collect, how they collect it, how they use it and what they will do with it/to whom they will disclose it. In addition, the OAIC has published guidelines in relation to the Information Commissioner's interpretation of the Privacy Principles and how they may apply in particular circumstances.

This approach to the privacy regulatory framework was deliberately adopted when it was drafted. The Privacy Act was drafted as principles-based law to ensure that its provisions were technologically neutral and could be adapted to new and evolving technologies. The ALRC in its *Report 108: For your information*, expressed its view that:

> *'technology-neutral privacy principles provide the most effective way to ensure individual privacy protection in light of developing technology. It would be undesirable to recommend significant changes to the UPPs to accommodate technologies, which are yet to be invented or deployed. Further where possible, provisions of the Privacy Act should be technology neutral.'* [4]

However, at the same time, the ALRC made clear that it did not recommend the adoption of a pure form of principles-based regulation. Rather, it indicated that in order to achieve the necessary policy outcomes, a pragmatic approach to the formulation of the privacy principles should be adopted, including by supplementation with more specific rules (either in regulations or other legislative instruments), to accommodate the particular needs and circumstances of different industries. It recommended a basic restructure of privacy regulation to follow this three-tiered approach:

- high-level principles of general application, provided in a streamlined Privacy Act;
- regulations and industry codes, detailing the handling of personal information in certain specified contexts, such as health and research, and credit reporting; and

[3] Digital Platforms Inquiry Final Report, p 384.
[4] Report 108: For your information, Chapter 10, 422.

- guidance issued by the Privacy Commissioner (and other relevant regulators), dealing with operational matters and explaining to end users what is expected in various circumstances, as well as providing basic advice and education.[5]

In coming to this conclusion, the ALRC considered (then) developing technologies including data-matching, data-mining, location detection and surveillance technologies amongst others and considered that a technology-neutral tiered approach to privacy regulation would best accommodate these as they developed as well as other new and emerging technologies.

It also noted the risk that, in order to operate effectively, a principles-based regulatory scheme requires the issuing of non-binding guidance that clarifies the rights and obligations contained in the primary legislation and their application in practice in specific contexts. It also highlighted the importance of research, monitoring and review by the regulator – to ensure that the primary legislation continues to operate as intended in the context of new and evolving technologies and data practices.

Similarly when discussing the broad and technology neutral approach to the Privacy Act in the context of the ALRC review, a number of stakeholders noted that the effectiveness of a technology-neutral Privacy Act will be dependent upon the technology-aware framework underpinning the legislation. For example, PIAC highlighted the important role of the regulator in a technology-aware privacy regime and the need for it to play a more proactive role in the exercise of its research and monitoring function with regard to the impact on privacy of new and emerging technologies. Similarly, the Australian Privacy Foundation also submitted that the overall privacy regulatory framework 'should be designed so as to ensure ongoing awareness of the impacts of technology, and to avoid blindness to them'.[6]

3.3 Approach to reform

In Free TV's view, the rationale for the existing tiered approach to privacy regulation, including a high-level principles-based Privacy Act, still stands and should be retained.

The key issue identified by the ACCC does not seem to be an issue with the first tier of the framework, but rather, with the next tiers that were envisaged would support the legislation to create a robust framework in the context of new and evolving practices. [7]

In many other cases, it would appear there has simply been inadequate incentive for the digital platforms to comply, even in areas where the intention of the law is fairly clear. For example:

- In the case of the scanning of content of Gmail accounts, Google essentially scanned the content of emails from over 425 million Gmail users and mined valuable information from those emails for commercial purposes. Google argued that this was not a breach of privacy because people do not have any 'reasonably expectation' of privacy in these circumstances and that the practice was 'ordinary business practice'. In this scenario, it was clear that the monitoring of personal messages, collection and use of information to deliver targeted ads and retention of data for an unlimited period, were not transparent to consumers.

[5] Report 108: For your information , chapter 10.
[6] https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol1.pdf at 422
[7] Digital Platforms Inquiry Final Report, p 439.

- In the case of the Cambridge Analytica issue, it was revealed that the company had access to the personal data of Facebook users which had been obtained from Facebook for purposes including targeted political campaigns of the first Trump presidential campaign and the Brexit movement. In this scenario, it was similarly clear that the use of consumers' data in this way was not transparent to consumers.[8]

In both of these examples, the Australian privacy regulatory framework provides sufficient foundation to deal with these issues. The actions of the digital platforms would be considered to be clear breaches of the Privacy Act. However, in both cases, the digital platforms were not sufficiently incentivised to comply with the law and seemingly took a 'risk-based approach' to privacy, to the detriment of consumers.

For these reasons, Free TV's view is that the most effective way to address the issues identified by the ACCC, is to:

A) strengthen the regulatory structures underpinning the Privacy Act including through better research of data practices, guidance on interpretation of the principles including how the law applies to these practices in specific circumstances, and

B) Ensure the OAIC is sufficiently resourced to effectively enforce the law so that organisations are incentivised to ensure their data practices comply, rather than addressing issues only once large-scale privacy breaches have occurred and been uncovered.

[8] Free TV submission to the ACCC, Digital platforms inquiry, April 2018, see: https://www.accc.gov.au/system/files/Free%20TV%20Australia%20%28April%202018%29.pdf

4. PART B – SPECIFIC AREAS BEING CONSIDERED FOR REFORM

In Part B of this submission we specifically address issues in relation to the existing provisions of the law and areas being considered for reform, including:

- the definition of personal information
- the approach to consent requirements, consumer defaults and notification requirements
- the exemptions
- a statutory cause of action for serious invasions of privacy; and
- direct rights of action to enforce privacy obligations.

4.1 Definition of Personal Information

In this section we set out why the definition of 'personal information' in the Privacy Act should remain unchanged.

4.1.1 Privacy Act should not deem specific types of data to be personal information

The ACCC's Final Report recommends the current definition of Personal Information should be updated to clarify that it captures technical data such as IP addresses, device identifiers, location data and other online identifiers that may be used to identify an individual.

Free TV strongly disagrees with this recommendation, as technical data on its own does not identify an individual. While it is essential that the Act regulates technical data collected from an individual's use of online platforms where an individual is identified or reasonably identifiable, the existing definition already does this.

The approach being suggested by the ACCC would tie the meaning of personal information to current technology, data types and uses. Firstly, this would bring purely technical data sets within the scope of the Act that otherwise wouldn't be personal information and should not be regulated. Secondly, it would move away from the technology neutral approach which has been recommended by the ALRC, as discussed in Part A of this submission. The definition of personal information should only cover information of any type or category when that information is about an identified or identifiable individual.

As outlined in Part A above, the ALRC has previously recommended against the ACCC's suggested approach and instead suggested that the application of the law in specific circumstances should be clarified via guidelines. The OAIC has already provided guidance on the issue of online identifiers and at what point data becomes personal information.

4.1.2 Digital identifiers

The application of the Privacy Act to technical information is not unclear. Technical data on its own does not identify an individual and therefore is not and should not be considered to be personal information.

However, where a digital identifier is used in a manner that does identify a person (for example, when stored with or otherwise connected to personal information), then it will be considered 'personal information' at that point. For example, if an individual logs into their online account and digital identifiers directly link to information that identifies them, the digital identifier will be considered to be personal information.

As noted on page 16 of the Issues Paper, the current definition of personal information already includes the requirement that personal information be associated with an individual that is "identified or reasonably identifiable".

In recommending the existing form of words in their report, *Report 108: For your Information*,[9] the ALRC sought to ensure that, whether a person is identified or reasonably identifiable must be 'based on factors which are relevant to the context and circumstances', and that the definition remained 'sufficiently flexible and technology-neutral to encompass changes in the way that information that identifies an individual is collected and handled'.

As the Issues Paper quite rightly notes, 'identifiability' captures a broader range of information than 'identity', including some online identifiers – if and when they are about a natural person. The existing OAIC Guidelines and caselaw on this issue are sufficient.

4.1.3 Inferred information

Similarly, the Privacy Act should not be amended to include "inferred information" as another category of personal information. Inferred information is not and should not be 'personal information' unless and until that information is about an identified individual.

The decision in the Ben Grubb case emphasized that there should be a requirement that personal information must be "about" an identified individual. Free TV strongly agrees with this. The possibility that information might be used to infer personal information regarding an individual should not be enough to make the information "about" an individual.

For example, a call center might maintain technical data regarding callers to its switchboard which, if examined, could be used to infer the calling behavior of callers generally, over time. However, that data should not become the subject of regulation unless and until the call center were to use its technical data to make inferences **about identified individuals**, at which point the inferred information would be "about" identified individuals. This is already the case under the existing regulatory framework and should continue.

4.1.4 De-identified, anonymised and pseudonymised information

De-identified, anonymised and pseudonymised information is not personal information. This information, by definition, does not identify individuals.

The ACCC has recommended that consideration be given to whether there should be protections or standards for de-identification, anonymisation and pseudonymisation of personal information to address the growing risks of re-identification as datasets are combined and data analytics technologies become more advanced.

While we agree that the OAIC should advise on protections and standards to ensure people understand when data is properly de-identified and the risks of re-identification, we do not consider that any amendments to the Privacy Act are required. Information that is capable of being re-identified would not satisfy the definitions of 'de-identified', 'anonymised' or 'pseudonymised'. When data is properly de-identified, it does not pose any security risks.

In addition, under existing privacy law provisions, APP entities are already required to de-identify or destroy personal information if they no longer need the information for any purpose for which it may

[9] Explanatory Memorandum to Privacy Amendment (Enhancing Privacy Protection) Bill 2012.

be used or disclosed under the APPs (APP 11). The Privacy Act also gives specific guidance on when personal information is 'de-identified'; it provides that personal information is de-identified 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable'.

The law in this area is therefore clear, however the OAIC should continue to provide guidance in relation to the risk of re-identification as technologies evolve.

Free TV notes that the ACCC appears to have taken a dim view on de-identification, however it should be recognised that de-identification is actually very good privacy practice, and that data in de-identified form is secure and poses no risk of harm to the individual from whose personal information it was originally derived. De-identification has significant security benefits, allows the creation and use outside the privacy regulatory framework of analytical and statistical information derived from personal information, and should also be seen as a legitimate alternative to deletion of personal information, where applicable.

4.1.5 Expansion of 'personal information' to cover groups

The suggestion that the definition of personal information might be expanded to cover households or groups of people when no one person is identified or reasonably identifiable (page 17) is strongly opposed.

The current position whereby personal information must relate to a living individual should remain unchanged. The relevance and utility of the privacy framework is that it helps to ensure personal agency and individual dignity. An expansion of the scope of the scheme to cover information that does not relate to a specific individual would be unnecessary and burdensome.

4.2 Consent to collection, use and disclosure of personal information

In this section we set out:

- Why the existing provisions of the Privacy Act relating to obtaining consumer consents are appropriate and why it would be counter-productive to increase existing consent requirements
- How the OAIC could play a greater role in promoting consumer understanding of collection practices
- How the existing notification requirements should be reduced to manage "consent fatigue", and
- Why the existing protections against unnecessary collection of personal information are effective.

4.2.1 Existing approach to consumer consents should be retained

Existing privacy law already provides a clear and appropriate framework in relation to when consumers' consents should be obtained and when they will be valid. Notably, the Privacy Act provides that consent means 'express or implied consent' and the OAIC's Australian Privacy Principles Guidelines provide that consent requires that:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- consent is current and specific;

- the individual has the capacity to understand and communicate their consent; and
- that consumers have a means of withdrawing their consent at any time.

Free TV therefore does not agree that existing laws need to be changed.

In Free TV's view it is important to draw a distinction between:

A. Practices which are not transparent to the consumer and where the consumer would not have a reasonable expectation that their personal information would be used or disclosed in a particular way; and
B. Practices which are transparent or where such a reasonable expectation does exist. For example, the collection of information necessary for the provision of a product or service and the use of information for delivery of that product or service.

This distinction already applies under our existing principles-based privacy law. Under APP 6, an entity can generally only use or disclose information for a purpose for which it was collected (the 'primary purpose'), however exceptions to this general rule apply where either the individual has consented to a secondary use or disclosure or where an individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection.

This approach should be retained. It is critical to ensure a pragmatic approach is taken to practices that consumers currently accept as standard, and where there are no significant privacy concerns, so that consumers' online experiences do not become unnecessarily clunky and slow. Many daily commercial interactions take place between businesses and customers without the customer giving any thought to or overt consent regarding the capture and recording of information by the relevant business. Any requirement imposing an additional legal step whereby customers are required to expressly consent to the collection of information is very likely to amount to a "click through" instance imposed by legal requirement that adds no value to either party.

Rather than increasing consent requirements, increased transparency through the publication of a privacy policy and the delivery, or other steps to ensure that the consumer is aware of certain matters at the point of collection or as soon as practicable thereafter, is a more reasonable framework that properly meets the objective of the Privacy Act by balancing the privacy of individuals with the interests of entities carrying out functions and activities on their behalf.

Keeping the circumstances in which express consent is required under the current regime will also help to minimise instances of "consent fatigue" and help to ensure that consumers treat requests for consent as useful and meaningful.

In this context it is also important to bear in mind that transparency is supported by other protections which benefit the consumer. In addition to ensuring that the data subject is informed by the privacy policy and a collection notification, the collecting entity is restricted regarding what can be collected by APPs 3 and 4; how the information can be used in accordance with APPs 6, 7, 8 and 9; is required to secure and, in good time, delete or de-identify the information by APP 11; and must facilitate access and correction of the information by APPs 12 and 13. For non-sensitive information the combination of transparency and these protections provides a framework that is practicable and workable without mandating express consent.

4.2.2 Pro-consumer defaults such as mandatory opt In

Free TV does not support a mandatory opt-in approach. However, if there is to be any move to a Mandatory Opt in Approach, it should be only with respect to practices which are not transparent to the consumer and where the consumer would not have a reasonable expectation that their personal information would be used or disclosed in a particular way. This might include provision of the personal information to a third party for the third party's own use, or targeted advertising on platforms outside the platforms of the first party collecting the personal information.

It should not be required with respect to practices which are transparent or within the reasonable expectations of the consumer, which might include targeting on the sites of the first party collecting the data, traffic measurement and analytics (for example Google Analytics which enables the measurement of traffic to websites). Customers reasonably expect when they visit a site that the site operator would be measuring traffic to the site and customer use of the site. They would also reasonably expect to be served targeted advertising on the sites of the party collecting the data based on their use of that party's site(s) (but not "off network").

By contrast, there is greater consumer concern in relation to online tracking and collection of personal information via Google's location tracking and Facebook's Onavo Protect VPN. Free TV notes that the GDPR similarly allows the processing of personal information where it is within the reasonable expectations of the user. It provides that the processing of personal data, where it is necessary for a company's legitimate interests or the legitimate interests of a third party, will be lawful unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

While Free TV favours a principles-based approach to law-making and does not think that the law itself requires strengthening in this area, the ACCC report does suggest that the current law is not being effectively enforced. The OAIC could play a role in this regard, to increase consumer understanding about the collection of data in exchange for the provision of free online content services. These practices in many instances have the potential to be of great benefit to consumers, and to provide a more relevant and targeted online experience. However, in order for consumers to consent to these services, they need to understand how their data is collected, for what purposes and how it will be used.

4.2.3 Notification requirements should be simplified to manage consent fatigue

In the final DPI report, the ACCC recommended strengthening notification requirements. In our view, this would be best achieved by ensuring that notification requirements are concise, clear and transparent. In this regard we agree with the ACCC that:

> *"The notice must be concise, transparent, intelligible and easily accessible, written in clear and plain language, provided free of charge, and must clearly set out how the APP entity will collect, use and disclose the consumer's personal information."*[10]

However, we strongly disagree with any suggestion that notification would be 'strengthened' by more complex or "multi-layered" notification requirements. Rather, it would be better achieved by ensuring that consumers are not provided with irrelevant information or any information that has already been made available. In other words, measures to ensure 'consent fatigue' is minimised, including by

[10] DPI Final report, Recommendation 16(b).

providing only necessary information in a clear but transparent way, will make both notification and consent more meaningful and strengthen the privacy framework overall.

4.2.4 Existing protections against unnecessary collection are effective

The requirement that information "other than sensitive information" not be collected unless it is reasonably necessary for one or more of an entity's functions or activities is a reasonable restriction that is understood and applied.

This restriction operates in the context of the mandatory data breach notification (MDBN) regime and the obligation to destroy or de-identify information that is no longer required for any purpose for which the information may be used or disclosed by the relevant entity (APP 11.2 (B)) and the consumer's right to access and correction of personal information under APPs 12 and 13.

The MDBN regime together with the APPs creates a positive incentive for businesses not to hold or collect unnecessary personal information. In the case of a data breach, the unnecessary information may give rise to additional onerous notification obligations and/or an investigation under APP 11 by the OAIC. Additional unnecessary information also must be disclosed to data subjects on request under APP 12.

4.2.5 Public interest disclosure

While we think APP 6/the existing requirements in relation to consent, use and disclosure are generally working well, consideration should be given to introducing a public interest exemption to allow for the use and disclosure of personal information where the public interest in disclosure outweighs the public interest in the individual's relevant privacy right.

This would allow access to more and better information on matters of public interest and would bring Australian privacy law in line with our defamation laws, which provide the defence of qualified privilege where an otherwise defamatory publication may be defensible because it is of public interest. This would be a logical alignment of the law given the Privacy Act regulates the handling of personal information, which is not disparaging, and which is true.

A public interest exemption to APP 6 would encourage transparency in Australia's public and private organisations and empower our journalists to pursue public interest journalism.

4.3 Journalism exemption

As indicated in the Consultation Paper, the journalism exemption is critical to maintaining a democratic society. Freedom of expression is a fundamental human right, as recognised by article 19 of the *International Covenant on Civil and Political Rights*, to which Australia is a party. The current exception recognises this and should be retained.

The journalism exemption at section 7B(4) of the Act, which exempts acts and practices of media organisations in the course of journalism, reflects a balancing of competing interests. Freedom of speech and the free flow of information that is critical to a healthy democracy on the one hand, and individuals' right to privacy on the other. This balance is achieved by only applying to those organisations that are publicly committed to standards that deal with privacy. These media organisations are bound by the privacy standards appliable to them and not the standards in the Act.

In the case of commercial television, broadcasters are subject to the strict standards contained in the *Commercial Television Industry Code of Practice*, which have been developed in accordance with the requirements of the *Broadcasting Services Act 1992*. These standards (clause 3.5 of the Code) prohibit the broadcasting of material relating to a person's personal or private affairs or which invade a person's privacy unless it is in the public interest or the person has consented to the broadcast. In addition, in the case of a person under 16, a parent or guardian must consent, and broadcasters are required to exercise special care, before broadcasting material relating to sensitive matters pertaining to a child's personal or private affairs.

Free TV does not support narrowing the exception. In Free TV 's view, the existing exception strikes the right balance between freedom of speech and individual privacy rights and generally works well. The requirement that media organisations must be subject to adequate standards effectively means that the exemption is already appropriately limited – it only applies to those media organisations that have appropriate standards in place. These standards prohibit reporting on matters that intrude on an individual's privacy except to the extent that such reporting it is in the public interest.

The existing privacy rules that apply to broadcasters are onerous and in some respects more onerous than under the Privacy Act, for example in relation to the rules that apply to children, broadcasting standards impose a stricter approach than the Privacy Act, which does not have different requirements for consent for children.

We do not support an approach of deeming when something is in the course of journalism and when it is not. That is a matter that should be determined based on all the relevant circumstances. Further narrowing of the exception is likely to exclude material that contributes to reporting in the public interest – for example, commentary on news and current affairs should not be excluded from the exemption.

We note that, if anything, consideration should be given to whether the journalism exemption should be broadened rather than narrowed. We note in this regard that in other jurisdictions such as the EU, acts and practices of media organisations other than those which are strictly in 'in the course of journalism', are also covered. In Free TV's view, to the extent that it is not, dramatised, documentary or entertainment content in the public interest should also be captured by the exemption.

4.4 Statutory cause of action

Free TV does not support a statutory cause of action for serious invasions of privacy. The current framework of legislative, common law and regulatory protections is extensive and generally working well. This framework includes: Commonwealth, State and Territory legislation (including in areas such as family law, evidence, children and young people, adoption, surveillance devices and many others); common law actions including breach of confidence, trespass, nuisance, defamation, malicious falsehood and contempt; and industry codes of practice. A statutory cause of action is therefore unnecessary.

Fundamentally, a statutory cause of action would fail to address the issues identified in relation to transparency of data practices and control for consumers that are unique to the relationships between consumers and the digital platforms that have been identified by the ACCC. A statutory cause of action would only provide a small number of individuals with sufficiently deep pockets the opportunity to pursue litigation after a privacy breach has occurred. For most people this would be meaningless. For the same reason, it would also be unlikely to incentivise platforms to improve their practices.

In addition, many of these concerns have been addressed by recent changes to the law to introduce a mandatory data breach notification scheme in Australia. The changes require government agencies and businesses covered by the Privacy Act to notify any individuals affected by a data breach that is likely to result in serious harm and are intended to improve transparency in the way that organisations respond to serious data breaches and to allow those affected to take practical steps to mitigate any harm caused.

A statutory cause of action would not only fail to address the issues identified by the ACCC, it would also risk an unjustified adverse effect on the freedom of the media to seek out and disseminate information of public concern. The ability to express opinions freely and access information about matters of public concern is a fundamental part of a free and open democracy and the media plays an important role in facilitating this information flow. A statutory cause of action would act as a deterrent to media companies reporting public interest stories due to the added complexity it would introduce to the privacy law framework and the increased risk of costly litigation.

It would place undue weight on an individual's right to privacy at the expense of freedom of communication. Free TV recognises that individual privacy rights are an important public interest. However, they must be balanced against other competing public interests including freedom of speech, which benefit society as a whole. This is particularly the case given that Australia doesn't have a clear process for balancing these rights in the form of a statutory human rights framework or express constitutional protection for freedom of speech (in contrast to other jurisdictions such as the UK and the US).

As such, Free TV's view is that there are no identifiable benefits to be achieved from introducing a statutory cause of action.

4.5 Direct rights of action

Similarly, Free TV does not support amending the Privacy Act to give individuals a direct right to bring actions and class actions against APP entities in court to seek compensation for an interference with their privacy. Actions such as these are generally not effective in addressing consumer concerns and are in practice available only to those with the resources to bring Court actions.

In addition, as outlined in 4.4 above, the existing dispute resolution mechanisms provide sufficient avenues for complaint – including individual consumer complaints to the OAIC – and these achieve satisfactory outcomes for consumers at a significantly lower cost than litigation. A better approach would be to ensure the OAIC is appropriately resourced to enforce privacy laws as outlined above.