UTS

CENTRE FOR MEDIA TRANSITION

Privacy Act Review

Issues Paper, October 2020

Submission to Attorney-General's Department

DATE: 28 November 2020

About the Centre for Media Transition

The Centre for Media Transition is an interdisciplinary research centre established jointly by the Faculty of Law and the Faculty of Arts and Social Sciences at the University of Technology Sydney.

We investigate key areas of media evolution and transition, including: journalism and industry best practice; new business models; and regulatory adaptation. We work with industry, public and private institutions to explore the ongoing movements and pressures wrought by disruption. Emphasising the impact and promise of new technologies, we aim to understand how digital transition can be harnessed to develop local media and to enhance the role of journalism in democratic, civil society.

This submission was prepared by:

- Dr Henry Fraser
- Professor David Lindsay
- Dr Sacha Molitorisz
- Professor Derek Wilding

Contact

Centre for Media Transition
Faculty of Law, University of Technology Sydney
Building 2, Level 15
UTS City Campus, Broadway
PO Box 123, Broadway NSW 2007

cmt@uts.edu.au
+61 2 9514 9669

cmt.uts.edu.au

Introduction

The *Issues Paper*[1] signals the first comprehensive review of Australia's data privacy law, the *Privacy Act 1988* (Cth) ('the Act'), since the release of Australian Law Reform Commission (ALRC) Report 108 in 2008.[2] While a number of recommendations from ALRC Report 108 were implemented in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth), many significant recommendations intended to address gaps and weaknesses in the data privacy regime were not, and must therefore be regarded as unfinished business.

The *Issues Paper* arose from a suite of recommendations for privacy law reform made by the ACCC in its *Digital Platforms Inquiry* (the 'DPI').[3] The DPI made it clear that, apart from the longstanding weaknesses with Australian data privacy law, the law had singularly failed to keep pace with evolving data practices and advances in data analytics, which characterise the business practices of the digital platforms, but which are not confined to the platforms. The Act is no longer fit for purpose, and requires fundamental reform to address both longstanding weaknesses and gaps exposed by rapidly changing technologies and business practices.

Since the release of ALRC Report 108, we have seen the development of global business practices revolving around capturing the attention of individuals, extracting data about them and their behaviour, aggregating this data, predicting preferences, traits and behaviour, and tailoring the presentation of information and services to individuals based on these predictions.[4] Increasingly, business practices are based upon the collection, aggregation and algorithmic analysis of large data sets. For entities such as search engines and social media platforms, '(e)very action a user performs is considered a signal to be analysed and fed back into the system'.[5] Signals such as views, 'likes', searches and buys are aggregated to create a profile of a user, and to group the user with other users with similar traits. Information presented to users grouped in this way – including advertising, search results and news feeds – is tailored for 'relevance' based on algorithmic signal analysis.[6] For example, different Google users may be presented with totally different search results for the same search terms, based on the way that Google has profiled them.[7]

Signal analysis by entities with access to large data sets may produce incredibly detailed information about individual users, without necessarily needing to directly identify them. For example, using only Facebook 'likes', researchers in one study were able fairly reliably to 'model' the latent traits of 58,000 volunteers, including sensitive traits such as sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, and substance addiction, among others.[8] Another study indicated that Facebook was able both to predict user

[1] Attorney-General's Department, *Privacy Act Review: Issues Paper* (October 2020) (the 'Issues Paper').

[2] Australian Law Reform Commission (ALRC), *For Your Information – Australian Privacy Law and Practice* (Report No 108, May 2008).

[3] Australian Competition and Consumer Commission (ACCC), *Digital Platforms Inquiry,* Final Report (June 2019).

[4] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).

[5] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt 2013), 113.

[6] Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You* (Penguin UK 2011).

[7] Zuboff (n 4).

[8] Michael Kosinski, David Stillwell and Thore Graepel, 'Private Traits and Attributes are Predictable from Digital Records of Human Behavior' (2013) 110 *Proceedings of the National Academy of Sciences* 5802.

emotions based on data analysis, and manipulate emotions through the newsfeed.[9] Given the resources invested into these techniques and practices, it is safe to assume that they are in the early stages of development, and that their sophistication and accuracy will increase. Significantly, the big data and algorithmic practices of entities such as digital platforms are largely opaque to end users, creating what has accurately been described as a 'black box society'.[10]

If Australia's data privacy law is to adequately fulfil its function of protecting the privacy and autonomy of Australians, it is essential for it to take into account the realities of contemporary data and algorithmic practices. The current reform process is therefore an opportunity to not only address historical problems with the data privacy regime, but to update the law to take into account contemporary realities, and establish a regime that reflects best practice. While some guidance in this may be obtained from what has emerged as the global standard, the European Union's *General Data Protection Regulation* (the 'GDPR'),[11] there is scope to learn from experience to build on and tailor the EU regime for Australian circumstances.

This submission does not attempt to set out a comprehensive response to the problems of adapting existing data privacy law to contemporary data and algorithmic practices. Neither does it attempt to address each of the 68 questions raised by the Issues Paper. Rather, it provides responses to selected questions which we consider especially important, and attempts to place these within the broader context explained in this Introduction. In addition to this, the submission suggests that it is important that, as illustrated by the DPI, data privacy law reform should not be seen in isolation from wider social and commercial issues raised by contemporary data and algorithmic practices. For example, data privacy reform should be seen as part of a coherent legal and policy response to related problems such as online harms, including (but not confined to) disinformation, the challenges facing journalism and the news media, and tendencies to increased polarisation of society and distrust among citizens. Establishing appropriate legal and technological protection of privacy and autonomy can assist with these problems by improving the trust that individuals have in their online interactions, and providing effective legal recourse for privacy harms.

It is important to make two further points: that breaches of an individual's privacy have the potential to harm not just the individual whose privacy is at issue, but also other people and, more broadly, society and democracy; and that alongside individual privacy there is group/collective privacy, which is also worth protecting. Indeed, in a networked society, it is impossible to conceive privacy in purely individual terms. Privacy is networked, collective and relational, which is particularly evident with social media. And although the Act currently applies to the privacy of individuals, it is increasingly important to take into account the relational or collective aspects of privacy. As the Cambridge Analytica scandal showed, for instance, when personal data about an individual is improperly accessed, that individual's voting intentions are vulnerable to being manipulated in subtle and hidden ways. This means that individual privacy violations can potentially compromise democracy, and society.[12] This is an example of the first

---

[9] Munmun De Choudhury et al, 'Predicting Depression via Social Media' (AAAI Publications, Seventh International AAAI Conference on Weblogs and Social Media, 2013); Robert Booth, 'Facebook Reveals News Feed Experiment to Control Emotions' *The Guardian* (30 June 2014).

[10] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2016).

[11] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC,* [2016] OJ L*1 19/1* ('GDPR').

[12] Sacha Molitorisz, *Net Privacy: How We Can be Free in an Age of Surveillance* (NewSouth Publishing, 2020) 181-182.

point. To give an example of the second point: as explained above, collected data may be aggregated to develop, by algorithmic inference, profiles of either an individual, or of an individual as part of a group. This will have implications for the regulation of both the sorts of data falling within the scope of the Act (eg. should group data be regulated?) and how data should be regulated. One specific area in which this may be increasingly important is whether there is a need for the regulation of inferred information about an individual as a member of a group. In general terms, we suggest that there are at least two distinct issues. One, how do we protect individual privacy in a way that adequately safeguards not just that individual, but also society and democracy? And two, how do we properly protect group/collective privacy? These issues require careful and ongoing consideration (and perhaps require a redrafting of the Act's objectives). However, they are not addressed in depth in this submission.

One final introductory point is that the Act has been inadequately enforced. Historically, this stems partly from insufficient funding for the OAIC. For the effective protection of privacy, extensive law reform is necessary. Also necessary, however, is that the OAIC is adequately funded and resourced.

Objectives of the Privacy Act

Question 1. Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?

Section 2A of the Act sets out eight objects that were each reasonable at the time they were introduced. Over the past twenty years, however, as outlined in the Introduction to this submission, there have been very significant changes in technologies and business practices. These changes give rise to a need for the objects of the Act to be revised and extended. Many of these business practices are associated with the activities of the digital platforms, and were the impetus for the DPI recommendation that the Government reconsider the objectives of the Privacy Act.[13]

To better reflect the realities of contemporary data practices, and to ensure that the Act remains relevant, we recommend that the objects set out in s. 2A should be clarified and extended in the following ways.

Amendment of current objects

Object (a): 'To promote the privacy and autonomy of individuals in accordance with Australia's international obligations to protect the right to privacy'.

Recasting the first object in this way would signal the importance of aligning Australian data privacy law with international best practice, including international human rights law. The Universal Declaration of Human Rights enshrines both a right to freedom from arbitrary interference with privacy (Art 12), and a 'right to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers' (Art 19). Given the ways personal data are now used to shape the ways in which individuals seek, receive and impart information and ideas, and form opinions, it is appropriate that the first object recognises the connection between privacy, autonomy and international obligations, especially human rights obligations.

[13] ACCC, *Digital Platforms Inquiry* (n 3) 477.

Moreover, the trans-border business practices of the global platforms make it especially important for Australia's data privacy law to be linked to, and to clearly reflect, our international obligations. Re-phrasing the first object to recognise the importance of Australia's international obligations would remove the need for the emphasis of this object in current sub-paragraph (h).

Object (b): 'To recognise that the protection of the right to privacy of people should be proportionate to other rights and interests'.

In the DPI, the ACCC concluded that 'it may be appropriate to reconsider the merits of balancing the right to privacy against the commercial interests of businesses that collect, use and disclose personal information'.[14] Rephrasing the second object as suggested would have a number of benefits. First, in accordance with Australia's international obligations, it would recognise privacy as a right which, while not absolute, merits strong protection. Secondly, it would incorporate what has increasingly been recognised as the international standard for rights-balancing, the 'proportionality principle', into the text of the Act. Thirdly, referring to the 'right to privacy of people' marks a shift away from exclusively protecting individual rights. Fourthly, it would recognise that the balances struck by the Act are not merely between privacy and the interests of entities that process personal information, but between the right to privacy and other rights and interests, including the right to freedom of expression.

Additional objects

(h) To promote the transparency of, and accountability for, automated uses of information relating to individuals.

This proposed new object is intended to address the realities of contemporary data processing practices, whereby large amounts of data are collected and processed in ways that are opaque to individuals that the data relates to. Such uses of information are increasingly automated, with consequences that materially affect individuals. Moreover, as explained in the section of this submission dealing with the definition of personal information, individuals may be materially affected even if the information is de-identified, inferred or aggregated. In order to satisfactorily protect the privacy and autonomy of individuals, in the face of automated big data practices, it is necessary to ensure that the practices are as transparent as possible, and that entitles are appropriately made accountable for the practices.

(i) To promote the privacy and autonomy of individuals materially affected by the processing of information relating to them, and especially by large-scale or automated processing.

In addition to promoting the transparency of, and accountability for, automated uses of information, there are other measures that are needed to protect the privacy and autonomy of individuals in the context of contemporary data processing practices. Some of these measures are identified in subsequent sections of this submission. To ensure that the Act remains relevant to the ways in which information is currently processed, it is important for this to be expressly recognised in the objects.

Definition of personal information

The definition of 'personal information' under section 6 of the Privacy Act establishes the scope of the information that is regulated by the data privacy regime, with information that does not fall

[14] Ibid.

within the definition being unregulated as it is essentially regarded as de-identified or anonymous. Issues have arisen with the scope of the definition, which were highlighted by the decision of the Full Federal Court in *Privacy Commissioner v Telstra Corp Ltd.*[15] In that case, the Court interpreted the requirement for information or an opinion to be 'about an individual', under the pre-2014 definition, as meaning that the individual must be 'the subject matter of the information or opinion'.[16] While the Court did not decide whether metadata, such as an IP address or URL, was personal information, by adopting a narrow approach to the definition, the decision has led to uncertainty about whether technical information, such as an IP address, is or is not personal information. This is because technical information, such as an IP address, may be interpreted as being 'about' a device, and not 'about' an individual, but in some circumstances could equally be interpreted as being 'about' an individual, in the sense that the individual is the 'subject matter' of the totality of the information.

Question 2. What approaches should be considered to ensure the Act protects an appropriate range of technical information?

Metadata that can be linked to an individual is highly revelatory. In practice, it is data such as an IP address or URL that are the primary means used by digital platforms to identify individuals. As the DPI concluded, the definition of personal information should be updated 'to align with consumer expectations and to reflect the realities of how data is used in digital markets'.[17] In addition, it is advisable for the definition of personal information to be amended to ensure consistency with international standards where, for instance, it is clear that under EU law technical information such as dynamic IP addresses that can be used to identify individuals falls within the scope of data privacy laws.

At a minimum, the definition of personal information under the Act should be amended so that the scope of Australia's data privacy law aligns with international standards. The simplest way to achieve this objective would be to adopt the definition from the GDPR, which defines 'personal data' as:

> any information relating to an identified or identifiable natural person.[18]

While this would go some way towards rectifying the deficiencies in the current definition, given the difficulties encountered by Australian courts required to interpret the legislative concept of personal information, it is likely that there would need to be more guidance about the application of the definition to technical information. For example, Recital 30 to the GDPR states that:

> Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

We therefore recommend that a mechanism be found to assist in the interpretation of the proposed new definition, so that it is clear that it clearly extends to information that may be used to indirectly identify an individual and information that can identify an individual when it is combined with other information.

---

[15] (2017) 249 FCR 24.
[16] (2017) 249 FCR 24, [63].
[17] ACCC, *Digital Platforms Inquiry* (n 3) 460.
[18] GDPR, Art 4(1).

Finally, in its submission to the DPI, the Internet of Things Alliance Australia pointed to the importance of taking into account the increasing amount of revelatory data collected by connected devices, including connected devices in the home.[19] It is therefore important that the protection of personal information under the Act clearly extend to information transmitted in machine-to-machine communications, including where there is no 'human-in-the-loop'.[20] In these circumstances, it is increasingly likely that there may be automated processes which affect individuals without there ever being a human decision-maker. Assuming that personal information communicated in this manner falls within the Act, there are clearly questions about how such interactions should be regulated, raising important issues of transparency and accountability.

Question 3. Should the definition of personal information be updated to expressly include inferred personal information?

Contemporary data analytics allows for inferences to be drawn about individuals from collected data, and some of these inferences may include inferred sensitive information, such as information about health, or religious or political views.[21]

We consider that the issue of inferred data is one of the most problematic features of contemporary data processing practices. For example, researchers have shown that seemingly trivial Facebook 'likes' can reveal political beliefs, drug use, sexuality and other highly personal characteristics.[22] Furthermore, more than half of those surveyed for the 2020 Australian Community Attitudes to Privacy survey conducted by the OAIC were uncomfortable with a business combining data about its customers (such as loyalty card transaction history) with other data (such as IP address) to better profile customers.[23] In addition, qualitative research reveals Australians are deeply concerned about the prospect of 'shadow profiles', a term describing how companies can use inferred and other data to build profiles of people who do not use their services.[24]

It is clear that the distinction drawn between personal information and 'anonymous' information has not kept pace with developments in data analytics, whereby highly sensitive details about an individual's life may be accurately inferred by aggregating multiple pieces of data which, in themselves, do not directly identify an individual. It appears that, under the GDPR, inferred data may sometimes be classified as personal data, but this is not invariably the case.[25] Where information is used to infer traits or preferences that have the character of sensitive information, there is a strong case for this inferred information to be regulated to the same degree as information that directly identifies an individual, especially given the widespread adoption of

---

[19] ACCC, *Digital Platforms Inquiry* (n 3) 460.

[20] See ongoing developments relating to the proposed EU *ePrivacy Regulation:* European Commission, *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/38/EC.*

[21] ACCC, *Digital Platforms Inquiry* (n 3) 479.

[22] Kosinski et al (n 8); *Issues Paper* (n 1) 19.

[23] *Issues Paper* (n 1) 19.

[24] Sacha Molitorisz and James Meese, *The Consent Trap: Australian focus groups on smartphones, privacy and consent* (Centre for Media Transition, University of Technology Sydney, 2020) 11.

[25] Bart Custers, 'Profiling as inferred data. Amplifier effects and positive feedback loops.' In Emre Bayamlioğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds), *Being Profiled: Cogitas Ergo Sum. 10 years of profiling the European citizen* (Amsterdam University Press, 2018) 112-115.

these practices. While this might be achieved by clarifying the definition of personal information, complexities arise in determining how best to regulate these common practices. As apparently suggested by the DPI, there is a need for further investigation of the appropriate protections and standards that should apply to inferred information.[26]

Question 4. Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?

In addition to the issue of inferred information, advances in data analytics have eroded the distinction between personal information, on the one hand, and de-identified, anonymized and pseudonymised information, on the other. As the DPI pointed out, there are increasing risks that information 'may become re-identified as more information becomes available, multiple datasets are combined, and advances in data analytics are made'.[27] These advances suggest that protection of data privacy should extend beyond the regulation of personal information to encompass the regulation of de-identification and re-identification technologies.

Under s. 6 of the Privacy Act, personal information is de-identified 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable'. It may be that the changes to the definition of personal information recommended in this submission would require changes to the definition of 'de-identified' information. Although the OAIC provides guidance on how to de-identify information, and how to manage and mitigate the risk of re-identification,[28] the risks posed by increasingly sophisticated re-identification techniques suggest that there is a good case for the Act to expressly incorporate enforceable principles or standards that apply to the de-identification, anonymization or aggregation of personal information. Furthermore, as explained later in this submission, the threats posed by powerful re-identification techniques further reinforce the need for the introduction of effective erasure rights.

Question 5. Are any other changes required to the Act to provide greater clarity around what information is 'personal information'?

As this submission has explained, contemporary data processing practices and advances in data analytics make it increasingly difficult to draw hard and fast distinctions between personal information, on the one hand, and de-identified or anonymous information, on the other hand. Furthermore, the courts are likely to continue to experience difficulties in applying this distinction to particular types of data or technologies. It is unlikely that any specific definition of 'personal information' will provide the necessary clarity to distinguish between information regulated by the Act and information that is not regulated, especially in the face of rapidly developing technologies and business practices, and in the face of the increasing prevalence of inferred data, as emphasised in this submission. There is therefore a need for a means of providing greater guidance on how the definition of personal information may be applied to particular forms of information or technologies. In addition to the guidance provided by the OAIC, we therefore suggest that there may be a case for delegated legislation made under the Act to expand upon the definition of personal information. This would enable the essential definition supported by this

[26] ACCC, *Digital Platforms Inquiry* (n 3) 479.

[27] Ibid, 480.

[28] Office of the Australian Information Commissioner (OAIC), *De-identification and the Privacy Act* (OAIC website, 21 March 2018).

submission, based upon the GDPR definition of 'personal data', to be flexibly clarified in its application to rapidly evolving technologies and data practices.

Exemptions

Small business exemption (Questions 7-12)

After a thorough review of the small business exemption, including stakeholder views, international experience and commissioned research, ALRC Report 108 concluded that 'the exemption for small business is neither necessary nor justifiable'.[29] In particular, the ALRC noted that the privacy risks posed by business do not necessarily depend upon the size of the business. In addition, the ALRC pointed out that removing the exception for small business would ensure the consistency of the application of privacy laws across the Australian economy and create greater harmony with international data privacy laws, including with assisting in achieving adequacy status with EU law.

Reduction in costs of data collection and processing technologies since 2008, and the increasing importance of data to all businesses, means that, if anything, the risks posed by small business are greater now than then. The exemption for small business has been a longstanding gap in Australia's data privacy regime – there is no equivalent in comparable jurisdictions – and we see no reason for the exemption to be retained. Although removal of the exemption would increase compliance costs for small business, it would also provide an incentive for small businesses to improve data management practices to the advantage of the businesses concerned. That said, if the exemption is removed additional support for small business will be needed to assist with their compliance with their data privacy obligations.

Employee records exemption (Questions 13-15)

When the Act was first extended to the private sector, it was envisaged that personal information in employee records would be dealt with in workplace relations laws. This has never happened. After a careful and thorough review of the advantages and disadvantages of removing the current exemption for employee records, ALRC Report 108 concluded that the exemption be repealed.[30] As noted by the ALRC, a major advantage of removing the exemption would be to better ensure the privacy of sensitive information held in employee records.

As with the small business exemption, the employee records exemption represents a longstanding gap in Australia's data privacy regime. And, as with that exemption, there is no equivalent exemption in the data privacy laws of comparable jurisdictions. There have been no developments since 2008 that would suggest that protecting personal and sensitive information held in employee records is any less important now than then. We therefore support the recommendation of the ALRC, in Report 108, to remove the employee records exemption, which has become increasingly anomalous.

[29] ALRC, Report No 108, [39.139].
[30] Ibid [40.121].

Political exemption (Question 16)

Political parties routinely use personal information, including by constructing voter databases for electoral purposes.[31] However, political parties, acts and practices are largely exempt from the Act. Section 6C expressly excludes 'registered political parties' from the definition of an Organisation; and s 7C exempts political acts or practices done in connection with an election, a referendum or another aspect of the political process by MPs and local government councillors, contractors and subcontractors for political parties and representatives, as well as volunteers for registered political parties.[32]

These provisions were drafted in 2000, well before big data, psychometric profiling and social media sought to harness personal data in an attempt to sway elections.[33] The most glaring attempt to manipulate the democratic process through the misuse of personal data was by Cambridge Analytica, as we have outlined above.[34] As a result of its role in the Cambridge Analytica scandal, Facebook was fined $US5billion by the Federal Trade Commission in the US. In Australia, the OAIC has launched legal action against Facebook Inc and Facebook Ireland in the Federal Court, alleging the social media platform committed serious and/or repeated interferences with privacy in contravention of Australian privacy law.[35] By contrast, it seems no action could be taken in Australia under the Act against any political parties, MPs, councillors, their contractors and subcontractors or volunteers if they engage in Cambridge Analytica-style practices.

In this light, it is unsurprising that there have been repeated calls to remove the exemption for political parties, acts and practices, including from the ALRC.[36] In 2019, in the lead up to a federal election, a group of privacy commissioners called for an end to the exemption following an online attack that left highly confidential records vulnerable.[37] As former NSW deputy privacy commissioner Anna Johnston said, '[The exemption] means not only that the political parties have no obligation to keep the data they hold secure, it also means we as citizens have no right to access the data they hold about us.'[38] We agree, and believe that registered political parties should not be exempt from the Act, and nor should political acts and practices. Given the risk to democracy, this would constitute important and timely reform.

Journalism exemption (Questions 17-19)

In general, the purpose of the exemption in s 7B(4), being rooted in the role of journalism in maintaining a democratic society, is even more relevant now that at the time it was introduced. Damage to the business model of news producers, the loss of local media sources, a loss of trust in institutions, and the proliferation of misinformation online are all reasons for strengthening the position of local sources of public interest journalism.[39] As the public interest in responsible

---

[31] Issues Paper (n 1) 33.

[32] Ibid.

[33] Molitorisz (n 12) 53-54, 63-62, 181-182.

[34] Ibid.

[35] OAIC, 'Commissioner welcomes ruling on Facebook application' (OAIC website, 14 September 2020).

[36] ALRC Report 108, Recommendations 41-1 – 41-4. See also, eg, David Vaile, 'Australia Should Strengthen its Privacy Laws and Remove Exemptions for Politicians', *The Conversation* (22 March 2018).

[37] David Crowe, 'Political Parties Should be Stripped of Privacy Act Exemptions after Hack: Experts', *smh.com.au* (18 February 2019).

[38] Ibid.

[39] See ACCC, *Digital Platforms Inquiry* (n 3).

interrogation of public and private figures and institution is as compelling as it was in 1988, there remains a need for a mechanism whereby this aspect of the public interest can, in appropriate cases, override the interests of protecting individual privacy. That said, a growing awareness of the importance of privacy, and changes in the media landscape, mean it is appropriate to review the terms of the journalism exemption. Below, we provide brief answers to the questions set out in the Issues Paper (beginning with Question 19), followed by further explanation.

Question 19. Should any acts and practices of media organisations be covered by the operation of some or all of the APPs?

Some acts and practices of media organisations are already covered by the APPs; only acts 'in the course of journalism' are exempted and we think that exemption should remain as a single exemption rather than (as has been suggested in the past) as a series of selective exceptions to specific APPs. However, the continuing operation of the single journalism exemption should be accompanied by a reasonable tightening of the terms of the exemption (which is the subject of Q16).

Question 17. Does the journalism exemption appropriately balance freedom of the media to report on matters of public interest with individuals' interests in protecting their privacy?

The exemption does not appropriately balance the freedom of the media to report on matters of public interest with individuals' interests in protecting their privacy because its replacement of the APPs with industry guidelines is not rigorous enough in its implementation. The term 'media organisation' should be narrowed. The requirement for a media organisation to subject itself to alternative privacy protections, suitable for newsgathering, should be strengthened and there should be a requirement for independent complaint-handling and decision-making. Beyond that, this review offers the opportunity for a more far-reaching opportunity for reform by introducing a cross-media standards scheme and making membership of this scheme a condition of access to the journalism exemption.

Question 18. Should the scope of organisations covered by the journalism exemption be altered?

The scope of organisations covered by the exemption should be narrowed to cover news organisations. While bloggers and other information providers complement the work of journalists, the case for extending the privacy exemption to them is not as compelling as the need to protect individual privacy.

'In the course of journalism', 'news, current affairs and documentary' and 'media organisation'

The definition of 'media organisation' needs review. Its inclusion of 'dissemination' suggests that a digital platform could qualify as a media organisation, although the scope is subsequently narrowed by the requirement that the protected activities are 'in the course of journalism'.

On the whole, we think the application of the exemption should be restricted to organisations (not individuals) that produce (i) news or (ii) current affairs (the term used by broadcast media) or comment/analysis (terms generally used by print/online). Further, the exemption should apply to them in relation to their newsgathering and associated content-making activities, but not in other regards (eg, it should not apply to the collecting of data on people who watch news programs online or who access online news sites). It should target professional journalistic activities, not the work of bloggers or other information disseminators; while bloggers and other sources

provide valuable additional information and perspectives, it is reasonable to restrict the carving out of the exemption to privacy obligations to trained journalists.

One option is to support the recommendations of the Office of the Privacy Commissioner (OPC) in its 2005 review[40] and the ALRC in Report 108 which called for a definition of 'journalism', and then to restrict the definition so that journalism is practised by professional journalists. Another is to leave journalism undefined but to narrow the category of those who can claim an exemption though their practice of journalism (ie, 'media organisations'). We favour the second approach, as we believe the exemption should apply to publishers, not individual journalists and that these publishers should be required to sign up to an independent, journalism-focussed privacy standard (as explained below). In any event, the definitions should not extend to information generally. We also think the category of documentary requires some consideration. It should not, for example, be as wide in scope as the following definition of 'documentary program' used in s 6 of the *Broadcasting Service (Australian Content) Standard 2016*:

> *documentary program* means a program that is a creative treatment of actuality other than a news, current affairs, sports coverage, magazine, infotainment or light entertainment program.

'Publicly committed to observe standards'

We see a number of problems with this element of the exemption.

1. The 'publicly committed' mechanism appears to require no more than a statement on a website. We do not understand the ALRC's proposition that, under the current provision, a media organisation 'must both expressly commit to observing the standards and evidence conduct of such observance' (1471). We think this approach demands review. On its face, it does not appear to require the media organisation to be a member of the group that has produced the standards or to subject itself to complaint handling and independent decisions on those standards (or to contribute to the costs of such a scheme). We think this is a seriously deficient aspect of the Act that undermines other aspects of the exemption. In our view, to claim the exemption, the media organisation must be either (a) automatically made subject to the standards by some legislative mechanism, as in the mechanism provided by s 123 of the *Broadcasting Services Act 1992* or (b) must become a member of an independent scheme that publishes privacy standards appropriate for journalism. Further, we think it would be desirable to harmonise the new approach to the membership standards schemes under this Act with other legislative schemes designed to promote media standards, such as the proposed News Media Bargaining Code.
2. In the past, criticism has been made of a lack of enforcement in alternative schemes, but we suggest it is the existence of independent decision-making and an independent complaints mechanism that should take priority over the enforcement arrangements. The published decision of an independent arbiter on whether the media organisation complied with the standards is itself a remedy for many complainants, especially in an environment where social media and other means of publishing and distribution mean these outcomes are more likely to be seen by others.
3. The standards themselves need improvement. In our view, the privacy protections established in the self-regulatory scheme administered by the Australian Press Council (applying to print and online news sources) are stronger than those approved by the

[40] Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005) 198, recs 58, 59.

ACMA in the broadcasting codes of practice. For example, clause 3.5.1 of the Commercial Television Industry Code of Practice applies only in relation to 'broadcasting a news Program or Current Affairs Program', not to the conduct of journalists and others in the course of newsgathering. The effect was highlighted in 2015 when the ACMA declared it had no power to act against the Nine licensees when a team from *60 Minutes* participated in an Australian woman's attempted abduction of her children in Beirut.[41]

4. We do not support the suggestion made in the past – including by the ALRC – that the OAIC should decide whether the media privacy standards are 'adequate'. However, we do think there should be some threshold of acceptability. We suggest the Broadcasting Services Act could provide a more forceful legislative mandate to require the codes to adequately protect privacy. In this case, in would be the ACMA that would make the decision not the OAIC, but it would do so against the background of its own guidelines and experience in balancing media freedom against protection of privacy.[42]
5. Beyond these suggestions, we have a more far-reaching proposal. In other policy statements and in research, we have advanced the idea that Australian news producers should be subject to a single media standards scheme for news and current affairs/comment and analysis that would apply across different platforms.[43] We have suggested that this scheme could be supported financially by digital platforms – important distributors of news – although they would not be required to observe the standards themselves as they do not engage in journalism. We have also suggested that membership of such a standards scheme would be voluntary, but any news organisation that did not join would not get the benefit of the exemption in s 7B(4) of the Privacy Act. We continue to believe this approach would help to lift media standards, remove platform-specific ambiguities, improve trust in news media more generally, and provide a more coherent and streamlined complaints path for consumers. We think the review of journalism exemption as part of the current review of the Privacy Act – being one of several pieces of an overall reform agenda initiated by the government – provides an opportunity to develop these ideas, and we note that at least Facebook has come some way towards accepting the concept of an industry forum in its proposal for a 'Australian Digital News Council'.[44]

Notice of collection of personal information (Questions 20-25)

The current paradigm for protecting personal information, embodied in the APPs, is by notifying individual data subjects and obtaining their consent to uses or disclosures. In the context of contemporary big data and algorithmic practices, there are real limitations on whether the 'notice-and-consent' model can protect personal information – and, in fact, by creating the illusion of autonomy and control, the model may well be counter-productive.[45]

---

[41] See Derek Wilding, 'The Scandal of 60 Minutes: No Broadcasting Standards, No Investigation' *The Conversation*, 1 June 2016.

[42] Australian Communications and Media Authority, *Privacy Guidelines for Broadcasters* (September 2016).

[43] See, for example, our submissions to the DPI and on the News Media Bargaining Code: https://www.uts.edu.au/research-and-teaching/our-research/centre-media-transition/publications/centre-contributions-policy.

[44] Facebook, 'Response to the Australian Mandatory News Media Bargaining Code Concepts Paper' (5 June 2020) 31.

[45] Woodrow Hartzog, 'The Case Against Idealising Control' (2018) 4(4) *European Data Protection Law Review* 423.

Research has suggested that the application of the notice-and-consent model to digital data is highly flawed.[46] Due to the attractions of convenience and 'consent fatigue', data subjects commonly agree to online terms and conditions, without there being any genuine consent.[47] More recent Australian research reveals that consumers recognise that consent often doesn't work; but also reveals that consumers do want notice-and-consent to work.[48] What this suggests is that there is a good case for strengthening the requirements for consent under the Act, but also for better recognising that, in the context of contemporary data practices, the notice-and-consent model must be supplemented by other measures to protect the autonomy of data subjects, and to protect society and democracy, as we argued in the Introduction.

Article 4(11) of the GDPR establishes a high threshold of consent, specifying it as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. The DPI unequivocally recommended similarly strengthening the notice-and-consent requirements under the Act. In particular, the DPI recommended:

- requiring 'all collection of personal information to be accompanied by a notice from the APP entity collecting the personal information … unless the consumer already has this information or there is an overriding legal or public interest reason';
- 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. Where the personal information of children is collected, the notice should be written at a level that can be readily understood by the minimum age of the permitted digital platform user';
- providing 'consumers with a readily understood and meaningful overview of an APP entity's data practices as a means of reducing their information burden, it may also be appropriate for these requirements to be implemented along with measures such as the use of layered notices or the use of standardised icons or phrases'; and
- 'strengthening consent requirements to require that consents are freely given, specific, unambiguous and informed and that any settings for additional data collection must be preselected to "off"'.[49]

We agree with the need to strengthen the requirements for notice-and-consent in order to ensure that the regime is more real than illusory. In particular, we agree with any regulatory measures that can reduce the information burden facing data subjects. As mentioned, however, given the inherent limitations of the notice-and-consent model, it is important that these measures be supplemented by additional safeguards.

First, privacy by design should be mandatory, as it is in the GDPR, and these provisions ought to direct designers to incorporate specific requirements for notice, including that it be accessible and easily understood. It is absolutely essential to understand the importance played by design in influencing the decisions of online users, including how design can undermine freely given consent. As Hartzog puts it:

---

[46] Daniel Solove, 'Introduction: Privacy self-management and the consent dilemma' (2012) 126(7) *Harvard Law Review* 1880.

[47] David Kravets, 'TOS agreements require giving up first born—and users gladly consent.' *Ars Technica* (13 July 2016); Peter Friedman, 'Should We Allow Consumers To Sell Their Souls?' *Techdirt* (19 April 2010).

[48] OAIC, *Australian Community Attitudes to Privacy (ACAP) Survey 2020* (OAIC website, September 2020); Molitorisz and Meese (n 24).

[49] ACCC, *Digital Platforms Inquiry* (n 3) 24, 461

> Design … nudges us by sending us signals and making tasks easier or harder to encourage us to act in predictable ways. Companies deploy 'dark patterns' to exploit our built-in tendencies to prefer shiny, colourful buttons and ignore dull, grey ones. They may also shame us into feeling bad about withholding data or declining options. They might simply make exercising control possible but costly through forced work, subtle misdirection, and incentive tethering.[50]

Secondly, standardised and simplified forms of notification ought to be provided, such as an initial summary with an outline of the data to be collected, proposed uses and on-sharing, purpose of collection, and how that data will be monetised. Thirdly, written notice-and-consent could be supplemented by other forms, such as concise audio and video versions. And fourthly, a standardised privacy rating, akin to the energy ratings on domestic appliances, while not a panacea, would enhance the clarity of notice provided.[51] On this point, we agree with the DPI suggestion in favour of layered notices and standardised icons or phrases.[52] In addition, any strengthening of the notice-and-consent regime must pay particular attention to the need to protect children and other vulnerable groups.[53] It is worth noting also that this is not an exhaustive list of additional safeguards.

Consent to collection and use and disclosure of personal information (Questions 26-31)

As explained immediately above, in the context of contemporary data and algorithmic business practices, it is important to recognise the limitations of the notice-and-consent model. While flawed, however, this does not mean that notice-and-consent is fatally flawed; and attention should be given to how to improve notifications, and ensure that consent is genuine and not merely illusory.

These conclusions are confirmed by recent qualitative research, referred to above, conducted by the Centre for Media Transition into consent, privacy and smartphones,[54] in which participants agreed that the current consent model isn't working. One participant described consent as 'a trap'. Without exception, however, they also said that they valued consent, and wanted it to work. To this end, participants made specific suggestions. They wanted notice-and-consent to be more sensitive to: vulnerable groups, including children; how people use technology, including the fact that multiple users may access one device; and the characteristics of smartphones, which have small screens and unstructured information. Further, they wanted informed consent to be: simple; clear; targeted; logical; relevant; real-world (with concrete examples); easily withdrawn; time limited; and re-obtained when apps change (with new features and data uses).[55] This list is not exhaustive, but points the way to what Australians want from consent, and indicates the need for a more robust and ethical model of notice-and-consent. The participants also expressed

[50] Hartzog (n 45) 427. See also Cohen, J. 2019. 'Turning privacy inside out.' *Theoretical Inquiries in Law*. 20(1), p. 1-32; Solove, D. 2020. *The Myth of the Privacy Paradox*. Working Paper, p. 40 Available at: https://scholarship.law.gwu.edu/faculty_publications/1482/,

[51] Eg, see tosdr.org; on these four points, see also Molitorisz and Meese (n 24).

[52] ACCC, *Digital Platforms Inquiry* (n 3) 35.

[53] Issues Paper (n 1) 38-9.

[54] Molitorisz and Meese (n 24).

[55] Ibid. 12-14.

frustration that the 'consent' process tended to be 'all or nothing'. That is, either agree and be allowed to access the service, or refuse and be denied. Participants wanted more options.[56]

This research reinforces our main responses to the questions raised in the Issues Paper relating to the notice-and-consent model. First, notice-and-consent cannot be seen in isolation, and it must be supplemented by other measures, especially ensuring that privacy by design is implemented as a fundamental principle of Australian data privacy law. Too often, the existing notice-and-consent model is undermined by design decisions that effectively render user consent meaningless. Secondly, as recommended by the DPI, the threshold for consent should be raised to match that in the GDPR so that, to be effective, consent must be 'freely given, specific, unambiguous and informed'. Thirdly, mechanisms should be established to ensure more effective communication of privacy notices to users, including the use of audio and video explainers, and privacy ratings systems. In themselves, none of these measures are a panacea to the problems plaguing the current notice-and-consent framework; but it is only by acknowledging the problem, and implementing a variety of mechanisms to address it, that progress can be made.

The role of consent for IoT devices and emerging technologies (Question 34)

The increasing popularity and prevalence of Internet of Things (IoT) devices poses significant challenges for data privacy laws, but also for consumer protection and data security. This development cannot be seen in isolation from contemporary data and algorithmic practices referred to in this submission. We agree with the statement made in the Victorian Privacy Commissioner's Issues Paper, that 'traditional methods used to protect privacy and better inform individuals about how their personal information is collected, used and disclosed are largely incompatible or insufficient for IoT devices'.[57] The issue addressed in Question 34, that IoT devices often collect personal information of multiple people, such as those in a household, without consent, raises challenges that are a difficult to satisfactorily address. Moreover, this example reinforces the observation made in the Introduction that privacy is increasingly networked, relational and collective.

The problem of unconsented collection of personal information by IoT devices can only be addressed by a variety of mechanisms, most of which have been mentioned in the previous section of this submission, in dealing with the limitations of notice-and-consent. First, it is important that the principles of privacy by design and security by design are applied to IoT devices, especially consumer IoT devices. While the voluntary code of practices for consumer IoT devices, released in September 2020,[58] is a positive step, it is a first step only. It seems doubtful that a voluntary code, in and of itself, will have the desired effect of properly securing IoT devices; and, in our view, there is a good case for mandating the principles in the code. Secondly, it is important that consumers are provided with accurate and truthful information about the data that is collected by IoT devices. This raises the need, identified above, for effective and innovative ways of communicating essential information to users, such as through audio and video explainers, and ratings systems. Finally, once information is collected, included information that is collected from people other than those who have consented, it is important

[56] Ibid 8-9, 17.

[57] Office of the Victorian Information Commissioner*, The Internet of Things and Privacy* (Issues Paper, February 2020) 11.

[58] Australian Government, *Code of Practice: Securing the Internet of Things for Consumers* (September 2020).

that data subjects are able to access the information and, as explained below, and subject to the safeguards mentioned, to have the right to have the personal information erased.

Control and security of personal information

Right to erasure

Question 46. Should a 'right to erasure' be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities?

Question 47. What considerations are necessary to achieve greater consumer control through a 'right to erasure' without negatively impacting other public interests?

APP 13 requires an APP entity to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading. Although 'reasonable steps' may require the deletion of personal information, this falls well short of providing data subjects with a right to erasure of personal information held by a third party.

Data privacy laws are designed to protect the right to privacy in the collection and processing of personal information, and to ensure the responsible management of such information by entities that hold or control it. As such, it is important for privacy laws to apply to the full data life cycle, and to establish appropriate rights over personal information at each stage of the life cycle. An essential part of a regulatory framework for protecting personal information is to ensure that, in appropriate circumstances, data subjects have rights to ensure that persona information is deleted or erased.

The DPI considered that establishing a right to erasure is an essential supplement to the other measures recommended for strengthening the privacy protections of individuals, such as improved notice provisions and a higher threshold for consent. This reform is especially important in the context of data management practices based on the mass collection of data, where the uses of the data are often determined or changed after the data have been collected and consent given, and where technologies allow for data to be re-identified. As the ACCC explained:

> The exponential increase in the number of data sets and technological developments in data analytics may … mean that personal information provided at one point in time could in future be used in ways not envisioned when consent was first given.[59]

In our view, it is not a question of whether or not a 'right to erasure' should be introduced into the Act – doing so would redress a longstanding gap in the coverage of the Act – but of establishing the conditions for the exercise of the right. On this, the DPI recommended that APP entities be required:

> … to erase the personal information of a consumer without undue delay on receiving a request for erasure from the consumer, unless the retention of information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason.[60]

[59] ACCC, *Digital Platforms Inquiry* (n 3) 471.
[60] Ibid 470.

As pointed out in the Issues Paper, the ACCC did not recommend introducing a mandatory deletion obligation on APP entities once information is no longer necessary for the purpose of collection, as this would impose too high a regulatory burden.[61]

Despite some alarmist commentary, the right to erasure in Article 17 of the GDPR has not imposed unreasonable regulatory or financial burdens on data processors nor, indeed, on the digital platforms. In accordance with fundamental principles of data privacy laws, entities that collect and hold personal information should be responsible for that information and, in some circumstances, that responsibility should extend to deleting or erasing the information.

We suggest that there are two main issues that need to be considered in introducing a right to erasure into the Act. First, there is the question of whether in addition to imposing an obligation to erase data on request (subject to countervailing considerations), entities should be under an obligation to erase data when it is no longer necessary for the purposes of collection. As a matter of best practice, the responsible management of personal information means that the information should sometimes be deleted. This is far and away the safest way to manage data that is no longer needed. We therefore support a general obligation to erase personal information where it is no longer needed; but note that, in order to deal with the costs imposed by such an obligation, it would need to be subject to exceptions, and might not apply equally to all entities.

Secondly, there is the issue of the circumstances in which the right to erasure might be overridden by public interest considerations. On this point, we agree that the right to erasure must be balanced against other legitimate rights and interests, and especially the right to freedom of expression. As pointed out in the Issues Paper, however, much depends upon how the right is framed – if it is limited to circumstances where the data subject withdraws consent or where the data is no longer necessary, then the conflict with other rights or interests may be minimal. That said, we suggest that the appropriate limits to a right to erasure is an issue that merits further discussion as part of the review process.

Statutory tort for invasion of privacy

Question 57. Is a statutory tort for invasion of privacy needed?

Question 58. Should serious invasions of privacy be addressed through the criminal law or through a statutory tort?

The Issues Paper refers to the various parliamentary and law reform inquiries into this issue and notes the consistent recommendation for a statutory cause of action for serious invasions of privacy. A cause of action has been supported by the Australian Law Reform Commission (twice), the New South Wales Law Reform Commission, the Victorian Law Reform Commission and the South Australian Law Reform Institute.[62] If anything, the case for a cause of action is strengthened as data collection practices expand and further instances emerge of misuse of private information. Meanwhile, the case for a cause of action for the less common but equally harmful instance of intrusion upon seclusion – provided it is accompanied by an effective means of recognising the parallel public interest in newsgathering – has not diminished.

[61] Issues Paper, 51.

[62] These were the ALRC Report 108; ALRC, *Serious Invasions of Privacy in the Digital Era* (Report 123, April 2014); NSW Law Reform Commission, *Invasion of Privacy* (Report 120, April 2009); Victorian Law Reform Commission, *Surveillance in Public Places* (Final Report 18, May 2010); South Australian Law Reform Institute, *A Statutory Tort for Invasion of Privacy* (Final Report, March 2016).

Accordingly, we think a statutory cause of action for *serious* invasions of privacy is needed. We think it should not to be implemented by way of criminal offence, with the criminal law reserved for appropriate specific matters such as image-based abuse. For the time being we will assume that the cause of action is a statutory tort, as opposed to a completely new cause of action, but we note that there may be reasons to identify two separate torts (intrusions into seclusion and misuse of private information), as recommended by the VLRC.[63]

We agree with the ALRC's view (expressed in Report 123) that it is preferable for this protection to be developed by way of legislation – which can address more directly the policy objectives associated with evolving technology – rather than through case law. In our view, developments since the ALRC reported (eg, improvements to protections for image-based abuse) – while worthwhile – are piecemeal and do not provide adequate cover for the range of situations in which there can be a serious invasion of privacy.

Question 59. What types of invasions of privacy should be covered by a statutory tort?

We agree with the ALRC that the cause of action should cover both intrusions into seclusion and misuse of private information. It should not be left more open-ended, as specifying these two elements provides more predictability in how the law will apply.

Question 60. Should a statutory tort of privacy apply only to intentional, reckless invasions of privacy or should it also apply to breaches of privacy as a result of negligence or gross negligence?

We support the ALRC's proposed objective test for a 'reasonable expectation of privacy', along with a statutory list of matters the court can take into account.

We do not support a strict liability approach, but we do think gross negligence should trigger the protection in respect of misuse of private information. We stress this should be 'gross negligence' not just negligence and we acknowledge the concept of 'gross negligence' may need a specific statutory definition.

Question 61. How should a statutory tort for serious invasions of privacy be balanced with competing public interests?

We acknowledge the ALRC's observation that, on its proposed approach, a public interest defence would not be necessary. This is because a plaintiff has the onus of establishing as part of the cause of action that the public interest in privacy outweighs any applicable countervailing public interest, such as freedom of expression and freedom of the media. We note that 'media freedom' was further specified by the ALRC as 'freedom of the media, particularly to responsibly investigate and report matters of public concern and importance' (150, Rec 9-2). On this approach, a defendant who wishes to raise a countervailing public interest must put evidence to this effect, but it is the plaintiff who has the burden of establishing that the protection of privacy outweighs media freedom or freedom of expression. The ALRC succinctly expresses the rationale for this approach as follows: 'A plaintiff should not be able to claim that a wrong has been committed—that their privacy has been seriously invaded—where there are strong public interest grounds justifying the invasion of privacy' (143).

We think that the need for news media organisations to be able to pursue public interest journalism – in an environment where important and legitimate investigative journalism faces

[63] See also, David Lindsay, 'A Tort for Australia? A Critical Appreciation of the ALRC Report on Serious Invasions of Privacy' (2015) January/February *Privacy Law Bulletin*, 8-11.

multiple and widespread legal restrictions and can be stymied by well-resourced litigants – means that the ALRC's approach represents an appropriate recognition of media freedom while also providing a mechanism for redress in the most serious cases. In general we support this approach, but we think the terminology relating to freedom of the media needs further consideration.

If, however, it is decided that the protection of media freedom should be included by way of a defence rather that as part of the cause of action, we think this defence should be wider in its protection of journalistic activity, and should be in addition to the more general public interest in freedom of expression. Since the ALRC reported, the Council of Attorneys-General has agreed upon a new defence as part of the Model Defamation Provisions which may provide some guidance. New section 29A will offer a defence where (a) the matter concerns an issue of public interest, and (b) the defendant reasonably believed that the publication of the matter was in the public interest.

In advancing this position, we have taken account of the multiple protections for news media that are already a part of the approach proposed by the ALRC, in addition to the burden placed upon the plaintiff to establish that their claim to privacy is stronger than any countervailing public interest. These include:

- the threshold harm test of seriousness
- the fault test of intention or recklessness, or potentially 'gross negligence'
- the requirement to establish there was a 'reasonable expectation of privacy'.

Question 62. If a statutory tort for the invasion of privacy was not enacted, what other changes could be made to existing laws to provide redress for serious invasions of privacy?

In respect of serious invasions of privacy by the media, if a statutory tort was not enacted, some improvement to the protection of privacy could be offered by making access to the journalism exemption in s7B(4) of the Act conditional on the media organisation subscribing to (not *committing* to) a standards scheme that provides adequate protection. In the case of broadcasters, this could be accompanied by a change to the Broadcasting Services Act that requires codes of practice to include a provision of this nature. A more far-reaching approach would be to establish a cross-media standards scheme, as we propose in our comments on the journalism exemption, above.