UTS

CENTRE FOR MEDIA TRANSITION

Privacy Act Review

Discussion Paper, October 2021

Submission to Attorney-General's Department

DATE: 24 January 2022

About the Centre for Media Transition

The Centre for Media Transition (CMT) is an applied research unit based at the University of Technology Sydney (UTS). Launched in 2017, the CMT is an interdisciplinary initiative of the Faculty of Arts and Social Sciences and the Faculty of Law.

The CMT works across disciplines to explore and develop: responses to the dramatic and ongoing movements wrought by digital disruption to the media industry; the role of journalism in Australia and the world; and the business models, ethical frameworks and regulatory responses that will best support a diverse and prosperous media.

This submission was prepared by

- Dr Sacha Molitorisz
- Dr 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

Suggested citation: UTS Centre for Media Transition, 2022. *Submission to Attorney-General's Department, January 2022, Review of the Privacy Act 1988 Discussion Paper.* Centre for Media Transition, University of Technology Sydney, NSW.

Introduction

The Centre for Media Transition welcomes the ongoing review of the *Privacy Act*, and thanks the Attorney-General's Department for the opportunity to respond to its wide-ranging Discussion Paper. In this submission, we respond to key points raised in the Paper and also address some significant general issues. It is structured in two parts: first, general responses; second, more specific responses presented in table form. This submission builds upon the more extensive and detailed Centre for Media Transition submission into *Privacy Act* reform completed in November 2020.[1]

1. General responses

i. The reform process is urgent and significant. As the Discussion Paper notes (p.2), the digital economy has brought immense benefits, partly thanks to technological developments enabling unprecedented collection of personal data. Unprecedented use of personal data, however, has also enabled extensive *misuse* of personal data, leaving individuals open to exploitation and making society and democracy vulnerable. Meanwhile, the regulatory landscape that seeks to protect privacy is complicated, confusing and piecemeal, leaving individuals under-protected and businesses and others confused as to their obligations. To better safeguard individuals, society and democracy, privacy needs to be protected much more effectively and coherently, and the current review process is a significant opportunity to take a step in the right direction.

ii. Privacy law reform to complement other law reform. Privacy issues are interconnected with many more digital media issues, including misinformation, hate speech, trolling, online safety, defamation and even public interest journalism. For instance, the proposed *Social Media (Anti-Trolling) Bill 2021* seeks to introduce a new process to deal with potentially defamatory content on social media, which includes digital platforms sharing the identity of certain users with complainants. Meanwhile, the news media bargaining code passed into law in 2021 contains provisions directing digital platforms to share data about news consumers with news media businesses. These regulatory innovations, among many others, are not primarily concerned with privacy, but have privacy impacts. Following the ACCC's Digital Platforms Inquiry, a number of reforms are underway or completed, on issues including misinformation, defamation and 'abhorrent violent material', among other topics. What's more, review of the *Privacy Act* is being accompanied by the development of an online privacy code. In recent years, there has been a torrent of law reform affecting digital media, with Australia sometimes pioneering world-first

[1] UTS Centre for Media Transition, 2020. *Submission to Attorney-General's Department, November 2020, Review of the Privacy Act 1988 Issues Paper*. Centre for Media Transition, University of Technology Sydney, NSW.

approaches. These reforms need to be undertaken in a way that is, as far as possible, coherent and complementary rather than contradictory, and to this end privacy needs to be seen in the broader context of digital data flows. A holistic perspective also stands a better chance of providing citizens with laws and regulatory mechanisms that are streamlined, consistent and hence *comprehensible*, rather than fractured and confusing.

iii. An approach aligned with international and domestic law. The Discussion Paper notes that many of the 200 submissions received favoured 'adopting particular definitions and obligations in order to ensure international consistency' (p.7). We strongly endorse this view. On 21 January 2022, the European Parliament voted overwhelmingly in favour of passing the *Digital Services Act*, which will include 'more transparent and informed choice' around targeted advertising, including clear opt-outs and tracker-free versions of online platforms. The draft law also includes a complete ban on serving targeted ads to minors. Australia is well-placed to draw on the best facets of overseas developments, such as the *Digital Services Act*. International consistency will give the best chance of effective enforcement, both here and abroad. Just as there have been warnings about the splintering of the internet (sometimes described as the 'balkanisation' of the internet, or the emergence of a 'splinternet') so too the splintering of internet regulation is to be avoided. A similar point concerns the inconsistent patchwork of laws that protect privacy in Australia at federal, state and local levels. The Discussion Paper noted that, 'Consistency with domestic legislation was also an area of concern [among submissions], particularly the lack of uniformity between state and with other Commonwealth legislation' (p.8). Here too, consistency is an important goal. This may involve the repeal and reform of laws other than the *Privacy Act*. On all these points, we note the significance of proposals in Sections 22, 23 and 28.

iv. The need for a law to protect *privacy*. The *Privacy Act* does not, in fact, protect privacy. Rather, it protects 'personal information' and 'sensitive information'. Amid the patchwork of laws that impact privacy in Australia, not one defines the term 'privacy'. This is a significant oversight. If we take seriously the value of privacy, then reform of the *Privacy Act* needs to be accompanied by the introduction of a legislated protection of '*privacy*'. This could take several forms, such as (to follow the UK) with the passage of a *Human Rights Act*. Australia *does* have a right to privacy, but that right is akin to a jigsaw puzzle that's only partially-completed and is missing many pieces. Currently, the right to privacy in Australia can be found in a piecemeal fashion in various regulatory instruments, rather than in any coherent legislative framework or provisions. The fundamental point is: given that breaches of privacy can compromise dignity, autonomy, relationships, society and democracy, Australian law currently has a major blind spot by not directly protecting privacy in any coherent way, and this ought to be remedied. This also makes the development of the online privacy code significant; further, the need for a coherent right to privacy underpins our support for the introduction of a statutory tort for invasion of privacy.

v. A principles-based approach. A considerable focus of privacy law internationally – including in the GDPR - concerns notice and consent. This was evident also in the Issues Paper, much of which was concerned with questions of notice and consent. We have argued elsewhere that notice and consent remain important, and that mechanisms of notice and consent need to be significantly improved.[2] However, we also agree with the many submissions to the Issues Paper arguing that an overreliance on notice and consent ought to be avoided (DP, p.7). Indeed, given the complexity and unpredictability of online information flows, other measures are vital. This includes foregrounding the role of privacy by design. It also involves strong law founded on principles. Law founded on general prescriptions, such as mandated fairness, mandated transparency, a prohibition on coercion and a prohibition on misleading and deceptive conduct have three major benefits: they leave interpretation to the courts; they can be intuitive, comprehensible and accessible, even for non-lawyers; and they are flexible enough to able to adapt to new technologies. General principles such as 'fairness' can be criticised for vagueness, certainly, but this flexibility is also a strength. Hence, for instance, we support proposals for the inclusion of a 'fair and reasonable' prescription as contained in Section 10 (see below).

vi. Even the best privacy law is powerless without adequate resources for enforcement. In many respects, Europe's GDPR of 2018 has set the benchmark for international privacy law. However, privacy remains a problem in Europe, with the vast majority of GDPR breaches reportedly unchecked and unremedied. Those infractions that are being identified and remedied are sometimes the result of work by not-for-profits such as the Austrian-based NOYB. In Australia, the Privacy Commissioner has been chronically underfunded. Reform of the *Privacy Act* (as well as other initiatives, including the development of a binding online privacy code) must be accompanied by substantial funding and resourcing increases that enable effective oversight. Privacy is a huge and growing area. Legal reform must be accompanied by much better resourcing for enforcement.

vii. The interconnected nature of our data and our privacy. Perhaps the biggest ongoing challenge for privacy law is that it seeks to protect individual privacy, but privacy is necessarily interconnected. If I upload details of my life to social media, I will probably also be sharing details about my family and friends, whether or not they have consented. What's more, the ability of social media to construct profiles of people who don't use their services is well-documented in research. This is largely due to inferred data, and hence privacy has been described as 'relational', 'networked', and 'collective'. On the internet, what I reveal potentially reveals you,

[2] Molitorisz, S., 2020. *Net Privacy: How We Can be Free in an Age of Surveillance*. NewSouth Books, Sydney; Molitorisz, S., Meese, J. and Hagedorn, J., 2021. 'From Shadow Profiles to Contact Tracing: Qualitative Research into Consent and Privacy. Law, Technology & Humans, 3, 46.

and vice versa. Inferred data is raised in the Discussion Paper, and looms as an ongoing issue. What if a social media company collects data about an individual that is not 'personal information' under the Act, but the volume of data held by the company enables it to infer with great accuracy various 'sensitive' attributes of that user? And what if that user does not use that company's services? The volume of digital data and the nature of the information economy means that companies can accurately profile and target people who do not use their services. Here, we do not have a complete answer to these questions. We commend the Discussion Paper for raising these issues, and want to underscore the point that a great deal more work needs to be done on determining how we, as a society, ought best to regulate the way that data can be inferred. Where do we draw the line? And how can we make sure we draw that the line is observed?

2. Specific responses to selected proposals

Proposal	**CMT Response**
1. Objects of the Act	We support the incorporation of the 'public interest' into the objects of the Act. However, we also submit that the objects ought to be expressed in a way that more forcefully underscores the goal of protecting privacy as a human right, in this case through the specific mechanisms of personal information and sensitive information. In this way, the objects ought explicitly to recognise that Australia *does* have a right to privacy, and that the *Privacy Act* is one component of that right. A more expansive account of our position is given in our Issues Paper submission. See also General Point iv above.
2. Definition of 'personal information'	We support several elements proposed, in particular: • We strongly support the proposal to change 'about' in the definition of personal information to 'relates to'. • We also strongly support expanding the definition of information to include 'inferred' information. As we note above in General Point vii, the issue of interred data will prove to be one of the ongoing challenges in any attempts to regulate data flows and to protect privacy. Protections against inferred data will need to be monitored and, in all likelihood, refined over time. We also support the proposal that data must be anonymous before it loses the protection of the Act, but note further that researchers have demonstrated that making data anonymous on the internet is extremely difficult, if not impossible.

	On the issue of 'sensitive information', we are sympathetic to the position taken by the Castan Centre for Human Rights Law, which (as summarised in the Discussion Paper) argues that 'the definition of sensitive information should be explicitly amended to include information that acts as proxies for sensitive information, because such proxies may be used as a basis for discrimination' (p.34). On the issue of biometric data, we note the trend among some companies and various jurisdictions to impose limits on the collection of such data, given the extent to which such data can reveal people. As the Discussion Paper notes (pp.34-35), the collection of genomic and DNA data by genealogy companies raises the prospect of such data being shared with third parties. This data then reveals not just the person who submitted the genetic data, but also relatives of that person. Clear legal parameters are required and we suggest regulators ought to err on the side of caution in terms of what is permitted. Facial recognition is another such issue, as revealed by the example of Clearview AI. Here, we support the Australian Human Rights Commission recommendation that legislation be introduced regulating the use of facial recognition and other biometric technology.
7. Journalism exemption	Here we respond to the final question posed in Section 7 on the journalism exemption: 'How could the self-regulation model for media organisations under the journalism exemption be improved?' We assume that the reference to 'self-regulation' includes the co-regulatory schemes operating under Part 9 of the *Broadcasting Services Act 1992* (Cth) (BSA) that are recognised as among the privacy 'standards' that a media organisation can publicly commit to under s 7(B) of the *Privacy Act*. A comprehensive answer to this question would require a separate program of work. Indeed, the Centre for Media Transition is nearing completion of research that reviews international literature as well as the regulatory arrangements in seven jurisdictions. The journalism exemption in Australia is just one aspect of this otherwise discrete topic of research, but there is a clear and important connection between the two topics: by making access to the exemption dependent on participation within a robust and accountable standards scheme – one that includes independent complaints-handling about news standards generally, not just privacy complaints – Parliament can help to maintain standards of reporting and promote alternatives to sources of mis- and disinformation. Although we have not yet completed our report, some aspects that emerge from this work are set out below. In general, we think

	it is important to restate the need for an exemption that recognises the civic function of journalism, while also acknowledging that the scope of this exemption should be limited to provide due regard for the equally important public policy objective of the protection of privacy. It is also worth stating at the outset that amending the journalism exemption without requiring something more than 'publicly committing' to unspecified privacy standards would render meaningless any reform of this aspect of privacy regulation. **Improving self-regulation** The following elements have emerged from our research to date on how an industry-based scheme for news standards, including privacy standards, could be made fit for the contemporary media environment. *Regulatory status*: some media standards schemes are statutory while others are fully independent of government. Some use a statutory connection without imposing statutory schemes. A statutory connection can be in the form of obligations (eg, a scheme will operate independently providing it complies with certain requirements) or entitlements (eg, access to defences or exemptions to other laws). In Australia, access to the journalism exemption could be made contingent on participation within an industry-based scheme that is not operated by government, provided it meets criteria such as operating a complaints-handling scheme that is independent of any specific publisher. *Coverage*: increasingly, news standards schemes are moving to a cross-media model that recognises the reality of the same news content appearing on multiple platforms operated by the same company. Australia lags far behind some jurisdictions on this aspect and there is a pressing need for reform. In our research report for the ACCC's Digital Platforms Inquiry, the Centre for Media Transition noted 14 different sets of rules about accuracy, fairness etc in operation in Australia in 2018, but this did not even include the platforms for which there were no rules for news content such as catch-up TV.[3] *Funding*: news standards schemes can be costly, particularly when they involve independent complaints handling as well as standards setting. Different approaches are taken to the financing of these schemes, with some jurisdictions opting for government funding and others leaving it to industry to finance. In Australia, industry funds the making of standards and at least initial complaint handling, but escalated complaint handling for

[3] Wilding, D., Fray, P., Molitorisz, S. & McKewon, E. 2018, *The Impact of Digital Platforms on News and Journalistic Content*, University of Technology Sydney, NSW, 88.

	broadcasting is performed by a government agency. In our submission on the Issues Paper, we noted that digital platforms could be brought into this aspect of the regulatory framework as associate members of a standards scheme; while not being required to observe publisher-specific obligations of accuracy etc, they could assist in funding the scheme. *Board composition and appointment*: an important aspect of any independent scheme is the appointment of public members in the governance of the scheme. Our research indicates that most schemes we reviewed appear to have an equal or higher number of public members. *Standards setting*: the scheme should set its own standards and not simply be given a complaints-handling role in relation to standards formulated by an industry group. The standards should be reviewed periodically and this should involve public participation rather than just consultation. The scope of standards also varies, with some schemes covering conduct involved in newsgathering, including claims of intrusion on seclusion, while other schemes cover published content only (as is the case for commercial television in Australia). *Complaint handling*: various approaches are taken to complaint handling, with early mediation built into some schemes, including through the use of a news ombud, before escalation to adjudication. Transparency of decision-making in terms of publication of outcomes and statistics varies among schemes. *Compliance and enforcement*: there is considerable variation in terms of the level of monitoring activity and especially in enforcement mechanisms. While some schemes, usually those with a more comprehensive statutory element, include financial and other penalties, some depend on publication of outcomes as the primary means of enforcement. See also General Point ii above.
8. Notice of collection of personal information	We support the improvement of notice requirements under APP 5. *Inter alia*, we support: • The introduction of 'an express requirement in APP 5 that privacy notices must be clear, current and understandable.' • Mandating that entities must specify: - 'the purpose(s) for which the entity is collecting and may use or disclose the personal information'

	- ‘the types of third parties to whom the entity may disclose the personal information’, and - ‘the fact that the individual may complain or lodge a privacy request (access, correction, objection or erasure)’ • The development of standardised privacy notices in an APP code such as an OP code.
9. Consent to the collection, use and disclosure of personal information	We support the proposal that consent be defined in the Act as ‘voluntary, informed, current, specific, and an unambiguous indication through clear action,’ which follows directly from the ACCC’s recommendation for consent that is ‘freely given, specific, unambiguous and informed’, which in turn follows similar wording in Article 4(11) of the GDPR. Such wording would render implicit consent inadequate, as in the form, ‘If you keep using this service, you will be taken to have consented to its data collection terms.’ We also support the development of standardised consents in the development of an APP code, such as the OP code, including ‘standardised layouts, wording, icons or consent taxonomies’, ideally developed in tandem with consumer testing.
10. Additional protections for collection, use and disclosure of personal information	We support the proposal that collection, use or disclosure of personal information under APP 3 and APP 6 must be ‘fair and reasonable’, including the non-exhaustive list of potentially relevant legislated factors to be taken into account to determine ‘fair and reasonable’. As noted in General Point v above, a principles-based approach built on notions such as fairness is likely to be able to adapt to new technologies, and is also likely to be clear and comprehensible for individuals, regulators and APP entities. The identification of ‘primary purpose’ and ‘secondary purpose’ are also likely to prove helpful. We agree with the analysis provided in the Discussion Paper case study (pp.89-90) that concludes ‘the sale of precise geolocation data by the weather application to data brokers is unlikely to be fair and reasonable in the circumstances’ under the proposed wording. We further submit that this is as it should be: an individual’s explicit consent for a weather app to collect precise geolocation data cannot fairly be taken to imply consent for the weather app to sell that data to brokers and other third parties, who are in a position then to on-sell such data. These proposals would hopefully go some way to curbing the trade in data obtained unethically, without meaningful consent.

	Similarly, we agree with and support the analysis of the second case study in this section (p.90), which concludes, 'The profiling of user moods and socio-economic status is unlikely to be fair and reasonable in these circumstances. An individual is unlikely to reasonably expect that a social media platform would infer these particularly sensitive traits without their knowledge.' The potential for harm to be caused by companies profiting from data that they are able to infer is great, and growing greater with advances in technology. We strongly support the introduction of a 'fair and reasonable' test for APP 3 and APP 6. As we argue above in General Point v, privacy law and the *Privacy Act* will benefit from the introduction of principle-based provisions built around notions such as fairness.
11. Restricted and prohibited acts and practices	We prefer Option 1 (entities identify and mitigate risks) over Option 2 (privacy self-management) given that the onus of compliance ought to be on the entities engaging in such practices, not on the individuals who are susceptible to such practices. What's more, Option 1 is more likely to foster both compliance and fairness.
12. Pro-privacy default settings	In line with the GDPR and academic research that supports privacy by design and pro-privacy as the default, we support Option 1.
14. Right to object and portability	We support this proposal, which provides that 'An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information.'
26. A statutory tort of privacy	The due protection of privacy in Australia requires the introduction of a statutory tort for invasion of privacy, and we endorse Option 1, for the introduction of a statutory tort as recommended by the ALRC Report 123.