Privacy Panel

Introduction

When, in June 2019, the ACCC published its final report in the Digital Platforms Inquiry, it made several game-changing recommendations regarding privacy law. Among the recommendations were that:

- the definition of "personal information" be updated to clarify that it captures technical data such as IP addresses, device identifiers, location data and any other online identifiers that may be used to identify an individual;
- notification and consent requirements be strengthened;
- APP entities be required to erase personal information on request;
- individuals be given direct rights to bring actions and class actions against APP entities to seek compensation for interferences with their privacy; and
- penalties be increased to the levels adopted in the Australian Consumer Law.

The ACCC also recommended that a broader review of the Australian Privacy Law be undertaken, which should consider:

- the objectives of the Act;
- the scope of the Act's applicability (including removing some of the exemptions);
- adopting a higher standard of protection, such as requiring all use and disclosure of personal information to be by fair and lawful means;
- better protecting inferred information, particularly where inferred information includes sensitive information;
- better protecting deidentified information;
- amending the Australian Privacy Law with a view to becoming "adequate" to facilitate the flow of information to and from overseas jurisdictions such as the EU; and
- introducing a third party certification scheme.

The ACCC further recommended that an enforceable code of practice be developed by the OAIC in consultation with industry stakeholders to enable proactive and targeted regulation of digital platforms' data practices. The ACCC recommended that the code should apply to all digital platforms supplying online search, social media and content aggregation services to Australian consumers and which meet an objective threshold regarding the collection of Australian consumers' personal information. The ACCC set out the sorts of requirements that it expected to see in such a code, including:

- requirements to provide and maintain multi-layered notices regarding key areas of concern for consumers;
- requirements to provide consumers with specific opt-in controls for any data collection that is for a purpose other than the purpose of supplying the core consumer-facing service;
- requirements to give consumers the ability to select global opt-outs or opt-ins such as collecting personal information for online profiling purposes;
- additional restrictions for processing children's personal information;
- additional requirements regarding security management systems;
- requirements to establish a time period for the retention of personal information that is not required for providing the core consumer-facing service; and
- requirements to establish effective and timely complaints-handling mechanisms.

The ACCC additionally recommended that Australia introduce a statutory tort for serious invasions of privacy.

Of those recommendations, the Federal Government expressed support for all except the erasure of personal information and a statutory tort for serious invasions of privacy. It noted both recommendations and said that they would need to be considered in the course of the general Privacy Law review.

In October 2020, the Attorney-General's Department commenced the broad review of the Privacy Act and, in October 2021, the Attorney-General's Department released a Discussion Paper, which addresses the issues above. And to help us make sense of what's being proposed, and the strengths and limitations in these proposals, we've assembled some of the leading privacy lawyers in our CAMLA community:

Katherine Sainty is the founder and team leader at Sainty Law. Katherine is a corporate and commercial lawyer who specialises in digital, technology and media law. A partner at Allens Linklaters for many years, Katherine gained significant experience advising clients from major technology, internet and media companies as well as Government departments and agencies.

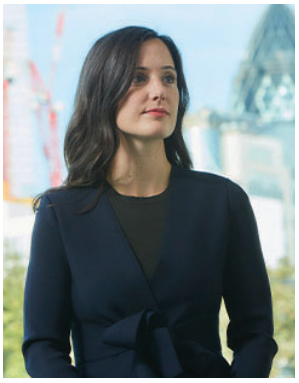
Sophie Dawson is head of Bird & Bird's dispute resolution practice in Australia and specialises in media, privacy and technology advice and disputes. A co-author of Thomson Reuter's *Media and Internet Law & Practice*, privacy law is a key part of her practice. Sophie has assisted high profile clients with submissions in relation to each of the privacy law reform processes since 2000, including the current reform processes. She regularly supports clients who have suffered data breaches, including across national borders.

Olga Ganopolsky is the General Counsel (Privacy and Data) at Macquarie Group, a role she has held since around the time the APPs were implemented. She was previously General Counsel at Veda (now Equifax), Australia's leading credit reporting agency and a provider of data to most of Australia and New Zealand's financial institutions. Olga's role typically involves giving advice on the privacy impact of new technologies, new acquisitions or restructuring businesses.

Anna Johnston is the founder and principal of Salinger Privacy, and one of Australia's most respected experts in privacy law and practice. Anna was the Deputy Privacy Commissioner for NSW and brings both a regulator's perspective to privacy law, as well as that of a private practitioner who has of wealth of experience dealing with clients' privacy and data governance challenges. Anna has been called upon to provide expert testimony before various Parliamentary inquiries and the Productivity Commission, spoken at numerous conferences, and is regularly asked to comment on privacy issues in the media. She is a lifetime member of the Australian Privacy Foundation, a member of the International Association of Privacy Professionals (IAPP) since 2008, and in 2019 was recognised as an industry veteran by the IAPP with the designation of Fellow of Information Privacy (FIP).

Ross Phillipson is a senior consultant in Norton Rose Fulbright's risk advisory practice. He provides risk and operational consultancy services with a focus on technology, data and cybersecurity. Based in Perth, Ross joined NRF after nearly 19 years working for global multinational Procter & Gamble in London and Geneva. From the end of 2012, Ross led P&G's European and APAC Data Protection, Privacy and Cybersecurity practice, guiding P&G through its GDPR and cybersecurity journey, as well as business tech law counselling and enterprise privacy and cybersecurity issues.

Rebecca Lindhout is a Special Counsel at McCullough Robertson. She specialises in procurement, technology, media and telecommunications, intellectual property and privacy and data-protection. Rebecca has acted for a broad range of clients including media and technology companies, for financial services providers including Big 4 Banks, clients in health care and aged care services as well as clients in the public sector. Rebecca was recently recognised by Best Lawyers Australia for Privacy and Data Security Law.



Ashleigh Fehrenbach is a Senior Associate at RPC in London, specialising in privacy and data law, intellectual property law, technology and brand protection. Ashleigh co-edits the *Communications Law Bulletin* and is firmly exercising her control over how much more I may embarrass her by singing her praises.

ELI FISHER: Thanks everyone for this. Let's jump right into the deep end. Let's talk notice and consent. One of the key themes of submissions following the Issues Paper was that transparency is essential. Another of the key themes was that we should be wary of overreliance on notice and consent mechanisms. There have been changes proposed to the APP5 notice regime and to the definition of consent. Can you talk us through those proposals?

OLGA GANOPOLSKY: The clear policy intent expressed by many of the contributors to the Discussion Paper is the need for greater transparency and a strong acceptance that individuals must make genuinely informed choices about the use of information that relates to them or is about them. Put simply, the driver is the need for agency. Without agency it is difficult to build a genuine case for legitimacy for the various uses of data and, in turn, trust in the data and the organisation seeking to use or otherwise process such data for commercial or other purposes. The complex debate now is *how* best to address this without compromising on the need for some flexibility and preserving technological neutrality. This is especially challenging a digital environment.

The Discussion Paper canvases ideas such as setting pro-privacy defaults, potentially on an industry basis, and/or for APP entities to provide individuals with a clear

way to set all privacy controls to the most restrictive by restricting the use of opt out mechanisms and instead replacing these with opt in mechanisms. It also seeks to remove some of the qualifications currently in APP 5.

We'll talk through the detail in the course of this discussion. The only rider I would add at this stage is that in considering the various options it will be important to test if they genuinely support agency, flexibility and technological neutrality. It would be, in my view, counterproductive to end up with a very prescriptive regime. This would not be conducive to agency of individuals or to the free follow of data, so critical in a digital global economy.

FISHER: Is trying to fix notice and consent a futile exercise in trying to improve something that is inherently broken? Should we be moving past notice and consent and pursuing other models of regulating the processing of personal information? In some respects, privacy law relying on transparency, notice and consent places the burden more on consumers than on companies. Is there a better way?

ANNA JOHNSTON: There is a role for notice and consent, but in my view that role should be limited. Consent, in particular, should be seen as the last option for authorising a collection, use or disclosure, rather than an entity's first or default position. Organisations should not be constantly asking customers to 'consent' to routine business activities, because then everyone just suffers consent fatigue. Consent should be kept for non-routine matters, like asking someone if they want to participate in a research project. Especially when you consider that the Discussion Paper proposes to tighten the legal tests for what constitutes a valid consent, by building into the legislation what has to date been guidance from the OAIC: that consent must be voluntary, informed, specific and current, and requires an unambiguous indication through clear action.

My reading of the Discussion Paper is that there is an intention to reduce reliance on the 'notice and consent' self-management model of privacy regulation, in favour of stricter limits on collection, use and disclosure. So instead of shifting the burden of assessing privacy risks onto consumers by asking for their consent to all sorts of practices, the Discussion Paper proposes that organisations must first apply a 'fair and reasonable' test before they collect, use or disclose personal information.

The proposal includes factors which could be legislated as relevant to any application of the test. The draft list includes things like whether or not a person would reasonably expect their personal information to be collected, used or disclosed in the circumstances; how sensitive the information is; what harm might come from it; and whether any loss of privacy is proportionate to the benefits. Plus, if the information is about a child, it must be in the best interests of the child.

This is a welcome suggestion, but in my view it still needs some strengthening. Otherwise I can imagine some tech platforms for example could argue that the kinds of revenue-generating algorithms which push harmful content in the name of 'engagement' are proportionate to the benefits of delivering free services.

Nonetheless, when you take the reform about the elements of consent, and add this new 'fair and reasonable' test, and then add in another proposal, which is to require 'pro-privacy defaults' when choices are to be offered to users, when combined these proposals should spell the end of companies using dark patterns to trick people into sharing their personal information in ways that end up harming us as individuals or collectively as a society, but then claiming 'consent' as their lawful basis for collection, use or disclosure.

KATHERINE SAINTY: Anna and Rebecca, below, have covered off what's being proposed very clearly. So, I wanted to focus on what this means for business. I see this as a critical change for the way Australian organisations do business online. Businesses are going to need to look very carefully at their privacy notices, collection statements and their online collection practices to make sure they stop using the default settings that many have adopted in the past. We've all been caught out with automatic opt in for marketing or cookies even though it's not permitted. The new standards for collection of personal data will be high: voluntary, informed, specific and current, with an unambiguous indication through clear action.

Businesses are going to have to rethink their marketing strategies and scrub contact lists so that they are only communicating with people who have actively opted in. They must refresh marketing lists regularly to keep consents current. There may also be some impact on secondary use of data so that if your business has collected information for one purpose it will need to rethink before it automatically uses it for another purpose. If the laws change, it will be a game changer for data miners as the focus shifts from monetisation to protection of data.

The Online Privacy Code is to detail on how Online Privacy Organisations must comply with the APPs in relation to policies, notices, and consents. Hopefully codification of the APPs in relation to policies, notices, and consents in the proposed Online Privacy Code, for Online Privacy Organisations, will catalyse good privacy practices from other businesses.

From a consumer perspective, I think it is likely that people will feel more comfortable with the new approach, as they will be able to see clear privacy messages. Consumers won't need to wade through multiple links, complicated and ambiguous notices and settings to work out how their data may be used without their knowledge or choice. Hopefully this will help to improve consumers trust and improve their relationship with businesses.

FISHER: Speaking of privacy by default, can you talk us through what this looks like? What's being proposed here, and how does that impact on businesses?

REBECCA LINDHOUT: As Anna noted, the most common approach at the moment is to provide individuals with information through privacy notices and policies – and then place the onus on the individual to manage their privacy through their choices. Pro-privacy defaults would instead result in pre-selections (set to 'off') – with the ability for individuals to then opt-in to further collection, use and disclosure of their personal information. Examples of pro-privacy defaults are the newer cookie pop-ups we're seeing from European companies where only 'strictly necessary' cookies are used unless you select otherwise at the point of entry to the website.

As is often the case with privacy legislation, pro-privacy defaults are a good example of how a one-size fits all regime is unlikely to produce a desired outcome. While a restrictive default collection and use regime might be appropriate if I am online shopping (and so help limit the targeted advertising I'm getting), it is likely to produce a less-than-ideal user experience in other contexts such as online services where information such as your location – or having your user profile visible to others - is key to the experience.

Accordingly, the Discussion Paper considers two options – one which requires pro-privacy settings by default, and the other which requires that they are easily accessible by individuals. In my view, a combination of Options 1 and 2 is likely to be most appropriate both in terms of ensuring the user experience isn't too cumbersome and ensuring that there isn't unnecessary restriction on online services offered by businesses. For example, Option 1 could apply to higher risk scenarios (such as where sensitive information or information relating to children is being collected, used or disclosed) with Option 2 applying to lower risk scenarios.

ROSS PHILLIPSON: I agree with Anna's statement that consent should be really considered as the last resort – in effect, the Privacy Act should build in gateways for processing personal information that society, via legislators, has decided are suitable and appropriate without needing consent. Assuming an entity has assessed and rejected these options, the only path forward is choice for the individual – i.e. consent.

For much of the criticisms that can be levelled at the GDPR, its six gateways for processing personal information, including contractual necessity, compliance with law and legitimate interests, in addition to consent, are a very useful framework in which companies and government agencies alike can determine the appropriate and applicable mechanism. In my experience, Europe has an unhealthy obsession with consent as the "gold standard"; and I fear the same will develop here in Australia. In my opinion, I'm not sure "fair and reasonable" actually achieves the counter-balance to an over-reliance on consent, particularly because what is one person's "fair and reasonable" is another's "unfair and unreasonable". I would rather see better defined alternate mechanisms that are distinct, rather than attempts at catch-alls.

My one major concern about pro-privacy defaults is the level at which they are applied. If the approach is not tailored at the relationship level, then the platforms as owners and gatekeepers of the connection with the end user may end up setting the standards, to the disadvantage of market participants. In effect, "owning the rails" enables these few companies to decide what those defaults are and, whilst it is not the role of privacy laws to combat the competitive impact, it is an unintended consequence that should be watched for closely.

FISHER: Thanks Ross. On that note, there are quite a few GDPRisms in the proposed set of reforms. Can you talk us through the GDPR influence here, and also where you think we've taken things even further?

ASHLEIGH FEHRENBACH: The Discussion Paper proposes a number of significant reforms to the Privacy Act, many of which as you've rightly pointed out Eli are based on the GDPR - the gold standard of international privacy regulations. If the changes proposed in the Discussion Paper are passed, this will represent quite a transformation of our privacy laws, particularly by bringing them more in line with the GDPR.

The GDPR type proposals include things like amending the definition of personal information, introducing a right to object and a right to erasure of personal information in certain circumstances. I don't intend to go into those individual rights and the proposed expanded definition of personal information here as I have a feeling we'll get to them later in this paper! However, outlined below are a number of instances where we see the Discussion Paper basing certain proposals on specific articles in the GDPR.

A GDPR-ism that we see in the Discussion Paper is around whether entities should be required to handle personal information in a fair and reasonable manner or in accordance with the 'legitimate interest' test. The legitimate interests test is contained in Article 11 of the GDPR. Broadly, it requires entities to 'handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.' The Discussion Paper considers that if this test were to be applied in Australia, a legitimate interests requirement would operate differently to the GDPR, in that it would consist of one factor to be considered within a broader test.

Another area is the conversation around an enhanced definition of consent. The GDPR requires consent to be a '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' (Article 4 (11)). The Online Privacy Code will, very similarly to the GDPR, require that consent be "voluntary,

informed, current, specific, and an unambiguous indication through clear action". The Online Privacy code will only apply to organisations that provide social media services, data brokerage services and large online platforms with at least 2.5 million end users in Australia (provided that the organisation is an APP entity). The Discussion Paper has recommended that the Privacy Act, which would apply to all APP entities (i.e more broadly than the Online Privacy Code), mirror the provisions in the Online Privacy code.

A further GDPR-type consideration in the Discussion Paper are data protection impact assessments (**DPIAs**). These are required under the GDPR (Article 35) for prescribed forms of personal data processing, including the large-scale processing of sensitive data, the large scale and systemic monitoring of a publicly accessible area, and personal data processing that is likely to result in a high risk to individuals. Rather than adopting the exact same approach under the GDPR, the Discussion Paper considers whether entities that engage in certain specified high-risk practices (or "restricted practices") should be required to undertake additional organisational accountability measures to adequately identify and mitigate privacy risks. Depending on that level of risk, an entity may need to conduct a formal privacy impact assessment.

Quite interestingly, there was some concern expressed in the submissions to the Discussion Paper about entities adopting a "tick box" mentality when undertaking privacy impact assessments. Some stakeholders were concerned that doing so may lead to a failure of entities to build privacy into the design from the outset of a project –which is the overall aim of a privacy impact assessment. This hesitance could be a learning from website privacy policies, which are sometimes drafted, published and never looked at again.

International approaches to regulating automated decision making (**ADM**) is a further example of where the Discussion Paper has looked to the GDPR for direction**.** The GDPR regulates the use of personal data in ADM systems 'which produce legal or similarly significant effects' (Article 22). At present, Australia's Privacy Act does not expressly regulate the use of personal information by ADM systems or otherwise regulate ADM. The Discussion Paper has proposed that APP entities be required to state in their privacy policies whether an entity will use personal information for ADM that has a legal or similarly significant effect. The aim of the proposal is to increase transparency about when an individual's personal information is used in ADM that affects them. This is an example of where technology has developed since the Privacy Act was enacted and Australian privacy laws need to catch up.

Additionally, age and consent is considered in detail in the Discussion Paper. The GDPR requires data controllers to make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over a child, taking into consideration available technology. In that regard, the Discussion Paper has suggested a change to the APP 5 notice obligations, requiring privacy notices to be clear, current and understandable and – importantly – emphasised in cases where the information is addressed specifically to a child. The proposed wording is modelled on Article 12(1) GDPR, i.e. "*The controller shall take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child*."

Despite what the above might suggest, the Discussion Paper does not by any means look at accepting the GDPR in its entirety. In fact, it reaches beyond the GDPR in a number of its proposals, for example the suggestion to create a direct right of action for individuals or group of individuals whose privacy has been interfered with by an APP entity as well as a statutory right for invasion of privacy. The UK deals with its direct right of action separately as claims for the misuse of private information, breach of confidence and/or breach of the GDPR / Data Protection Act 2018.

The Discussion Paper also refers to approaches adopted in countries with GDPR adequacy such as Canada and New Zealand. The requirement for consistency with other jurisdictions is justified in the paper to better facilitate cross border transfer of information, a necessary requirement in today's digital economy.

PHILLIPSON: There is little I can add to the substantive review provided by Ashleigh above, so I will focus on one element that I think is of strategic importance to how Australia's privacy laws develop in the near future – whether or not adequacy with Europe is a strategic goal. I raise this as I am not sure Australia should focus on adequacy as a goal, or whether we should seek to develop a privacy regime that takes the best from around the world, including Europe, whilst avoiding the mistakes, and adapting the principles to promote a balance between the protection of individual privacy rights and the growth of digital business and innovation in Australia.

If it is the latter, there is nothing that would prevent Australia from doing so and still achieving adequacy without adopting GDPR standards wholesale. This has been achieved in other jurisdictions such as Switzerland and given our unique global position, we may be better suited to looking towards other jurisdictions as well and ensuring our access to those digital markets is facilitated rather than necessarily focussing on European adequacy.

OLGA GANOPOLSKY: Just picking up on Ross's comment, in my view adequacy, or a similar form of recognition, provides APP entities with an economy wide mechanism to transfer personal data without the need to implement measures (such as Standard Contractual Clauses or Binding Corporate

Rules) at an entity or enterprise level. This is a significant benefit for those looking to cut red tape and especially for organisations that have a global footprint and regularly transfer personal data across borders. Noting that many of our neighbours and trading partners already enjoy the benefits of adequacy, (e.g. NZ and Japan) the current reform presents a good opportunity to update the Privacy Act to enable, or at least not to be an impediment to, a successful application should the decision be made to apply for adequacy in the near future.

FISHER: There is a special concern regarding the processing of the personal information of children. What's being proposed here, and do you think it's the right approach?

LINDHOUT: There are a number of proposals in the Discussion Paper which specifically address personal information relating to children and would see personal information relating to children given additional protections.

The first of these addresses who is able to provide consent in relation to the collection, use and disclosure of personal information relating to a child. The Discussion Paper proposes a baseline requirement for parent or guardian consent for people under the higher age of 16 (current OAIC guidance uses 15 as the default age). This age may also be the relevant age for determining whether a child exercise their privacy rights – including access, correction or erasure requests, independently.

Adopting a threshold of 16 would mean alignment with the age (under the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (**Online Privacy Bill**) – discussed further below) under which parent or guardian consent is required by social media services. In my view, a statutory position on the relevant age for a child to provide consent is a useful starting point, although I think that there should be room for APP entities to show that consent has been provided by a younger person in appropriate circumstances to ensure that the regime does not become unnecessarily restrictive. For example, consent may be able to be provided by a younger person where there is an ongoing personal relationship such as with a teenager's GP in the healthcare context, or where the nature of the personal information doesn't demand such maturity to provide consent.

The Discussion Paper also proposes a change to APP 5 so that collection notices are required to be clear, current and understandable, in particular for any information addressed specifically to a child. It is likely that the reforms will see changes to the way all collection notices operate so that they are able to be understood by the relevant audience, so this change feels consistent with the overall changes regarding informed consumers and valid consent.

Another of the proposals in the Discussion Paper is that there should be legislated factors to be taken into account in determining whether the collection, use and disclosure of personal information is fair and reasonable in the circumstances (i.e. for the purposes of the changes being considered in relation to APPs 3 and 6). One of the recommended factors is that where personal information relates to a child, that collection, use or disclosure is *in the best interests of the child*.

From the APP entity's perspective, although this wouldn't prevent commercial entities pursuing commercial or other interests, it's unlikely that commercial interests would outweigh a child's right to privacy.

From the consenting parent or guardian's perspective, while the concept of 'best interests of the child' sounds great in theory, and goes some way to avoiding a scenario where a parent or guardian provides consent which is for their own benefit and not of that of the child (e.g. where does the line lie between allowing the collection and use of phone location tracking which is for the safety of the child rather than snooping purposes). This is something that APP entities should keep in mind where getting parents/guardians to consent on behalf of their child.

The Discussion Paper goes on to consider options for managing certain 'restricted and prohibited acts and practices' including the collection, use or disclosure of children's personal information on a large scale – having regard to the 'best interests' test. Some submissions in the process so far have proposed 'no-go' zones such as the profiling and behavioural advertising knowingly targeted at children. The paper notes, however, that straight prohibitions may reduce beneficial and legitimate practices which pose little or no risk - such as the algorithm within Spotify that helpfully provides recommendations for my daughter based on her previous listening habits and puts us into a Wiggles and Disney loop.

Accordingly:

- Option 1 of the paper proposes that if an APP entity proposes to undertake such activities, they must take reasonable steps to identify privacy risks and implement measures to mitigate those risks – presumably this would take a similar form to privacy impact assessments which are now commonplace in Europe.
- Option 2 would see those risks being self-managed by the relevant individual.

It is unclear how Option 2 would operate where the relevant individual is a child and so is unable to provide meaningful consent themselves – instead it will likely impose additional burden on parents and guardians – which may be impractical in online settings particularly where the child doesn't seek parent or guardian consent. Provided that there is sufficient guidance around what reasonable steps are, and that the efficacy of those assessments is subject to review and assessment, Option 1

seems a more appropriate option as regards the protection of children in particular.

Other changes under consideration which indicate the additional protections to be provided to the personal information of children include:

- the fact that one of the limited circumstances in which a right to request the erasure of personal information is where the personal information relates to a child and the erasure is requested by a child, parent or authorised guardian; and
- the 'pro-privacy' default settings as they apply to children's services – including particular features/functions which should be disabled by default in relation to children such as their geo-data and the ability for services to share their personal information.

FISHER: These reforms will likely be the most major privacy reforms since the introduction of the APPs in 2014, and may even exceed that round of reforms in consequentiality given how the data economy has matured since then. So much has changed in that time in the ways that businesses – especially digital platforms – are using data. As the data economy evolves, what confidence can we have that these news reforms will be fit for purpose going forward?

SOPHIE DAWSON: The current regulatory changes are being considered in the middle of a time when the industry is finding new ways to manage privacy risks for individuals, for example, Apple's iOS 15 now provides users of Apple devices true anonymity in relation to third party cookies and software development kits (**SDKs**).

However, it does bring comfort that the Attorney-General's Department is undertaking extensive industry consultation as part of its review and that it has noted the "general view among submitters" that flexibility, industry-neutrality and technology-neutrality are key benefits of the APPs.

This is an important opportunity for media, IT and telecommunications companies to explain to regulators the various issues that could arise from various proposed reforms.

The issues also have wider importance for us as a society. There are important issues at play. Unlike defamation law, which regulates false and damaging speech, privacy law affects the ability to make communications which are true, even when the information is not in any way damaging. The important role which freedom of communication has, particularly in the media sector, in ensuring the integrity of our key institutions including courts, government and companies, needs to be firmly borne in mind when tailoring a path forward. Our clients in the IT sector also remind us that it is important to bear in mind Australia's interest in having a key place in the global information economy, which means that regulators need to think about the impact of the different approaches on the willingness of entities to store data, and base digital businesses, in Australia. The same is true in the research sector including in areas like AI, where changes in the definition of personal information or in the approach taken to de-identification could have a substantial impact. All of these different considerations need to be carefully considered and balanced when considering the right level of, and approach to, privacy protection in Australia.

SAINTY: Australian business has struggled with a privacy regime that does not meet the GDPR standards of adequacy. This makes it hard for Australian organisations to do business internationally, or even for Australian-based businesses to manage cross border data restrictions. We know that part of this phase of privacy reform is to bring the law in line with GDPR, which would help bring us in line with international standards. Putting the data economy to one side, this aspect of the reforms is a significant step in making Australian privacy law fit for purpose going forward.

The digital landscape is highly dynamic, and the way people are engaging and interacting online is changing, particularly in the last two years with the impact of COVID-19. This means more people are taking advantage of technology to work from home. More people use ecommerce for transacting business and, domestically, for goods, services and information.

I don't think we have yet seen the full effect of how this will change the way the data economy works. Privacy regulators are going to struggle to keep pace with the rate of change. Laws need to be sufficiently technology neutral and industry neutral to cope with that change. As more cross-industry collaboration and innovation happens, business is finding more creative ways to collect and use consumer data. So, having flexible, technology neutral principles that can cover these innovations is crucial.

There is always a tension in finding the balance between protecting individual privacy, allowing businesses to run effectively and economically, and the protection of other public interests such as public health and safety, national security, freedom of expression. The APPs currently allow for flexibility, not prescription, in the way organisations apply them. We have seen them applied inconsistently and consumers receive different levels of protection. The Discussion Paper is moving the Privacy Act to a place of more clearly articulated requirements for the protection of the privacy of individuals, with a balancing concept of public interest.

One of the key challenges to date has been that the OAIC has not been taken as seriously by business as some other regulators. Things would change radically if the Information Commissioner were given the powers proposed in the Online Privacy Bill which would align it with regulators like the ACCC. Of course, the OAIC would need to have a commensurate extension in funding to realise the potential of the legislation.

FISHER: One of the most key changes being proposed is to widen the scope of the Privacy Act, both by amending the definition of Personal Information, and by removing exemptions. Let's start first with the definition of Personal Information, and address the exemptions in a sec. Can you take us through the issues around the definition of PI?

JOHNSTON: By amending the definition to cover information that "relates to" an individual, instead of the current test which is "about" an individual, the proposed reforms will address some of the confusion caused by the *Grubb v Telstra* line of cases, as well as bring the Privacy Act into line with the newer Consumer Data Right scheme, and the GDPR. This is good news.

Another welcome development is a proposed list of what will make someone 'identifiable', with examples including location data, online identifiers, pseudonyms, and other factors specific to the identity or characteristics of a person.

Critically, the Discussion Paper states that the new definition will cover circumstances in which a person can be distinguished from others, despite not being named. This is a very important and positive development, to help address the types of digital harms enabled by individuation – that is, individualised profiling, targeted advertising or messaging, and personalised content which can cause harm, but which currently escapes regulation because organisations can claim that they don't know precisely who the recipient of their messaging is. This development will have significant implications for digital platforms and social media companies, as well as the AdTech and data broking industries.

PHILLIPSON: I'm not entirely sure I agree with Anna that this is a good development. It is important to remember that this is the most important definition for determining the application of the Act. If the information is not personal information, then the Act does not apply. If it is, then it does. Given the substantial regulatory burden and the slated increase in penalties to $10 million or 10% turnover for breaches, it is critical that the definition of personal information is both technology agnostic, but also clear.

From my perspective, there are significant unintended consequences of such an expansive definition of the single trigger for the application of the Act. The largest by far is just the sheer increase in data management and processing that will be covered by the Act and the regulatory burden that will entail, especially when combined with other changes such as the right to be forgotten, access and correction.

Further, the justification given, relating to addressing digital harms caused by individuation appears to me to expand the ambit of privacy law into consumer protection law. I think it would be preferable to address consumer protection and digital harms via laws specifically designed to deal with those, whether an individual is known or "only" singled out, rather than expanding the definition of personal information in such a manner.

DAWSON: These changes could have very significant impacts in a large range of contexts, and it is important for each sector to carefully think through them. In the AdTech environment, it means that practices currently treated as being outside the scope of the Act will squarely fall within it. There are concerns that this will require a variety of new notifications and consents, which could actually require more personal information to be collected in some circumstances. TMT companies need to be thinking about the impact these changes could have on their systems, processes and practices so that they can identify and communicate any concerns as part of the reform process.

FISHER: How are the changes proposed to deal with anonymous and deidentified information?

JOHNSTON: There's always a language problem here, because 'de-identified' means one thing to data scientists and statisticians, and another thing to lawyers. In law, it means that information has been treated, and the access environment controlled, in such a way that no individual is reasonably identifiable from this data, alone or in combination with any other data. That's a much higher standard than just 'oh well we stripped out the direct identifiers', or 'we used hashed emails to match up customer records'.

The Discussion Paper proposes to make this clearer. The proposal is to incorporate a definition that makes it clear that, to apply de-identification such as to fall outside the scope of the definition of 'personal information', an organisation must meet a test which is that there is only an "extremely remote or hypothetical risk of identification". It will also make clear, like the GDPR does, that pseudonymised information is still 'personal information'.

However, I believe that still leaves a gap between the test arising from the definition of personal information – which is effectively "not reasonably identifiable" - and the test in the proposed definition of de-identified data – which is "extremely remote or hypothetical risk of identification". This gap creates a legislative no-man's land of data which is not personal information in scope but nor is it de-identified and out of scope.

There should not be any gap between the two. The line between identifiable and not should be based on the "extremely remote or hypothetical risk of identification" test. Otherwise bad actors will continue to argue that because no one is 'reasonably' identifiable in their data, they are not regulated by the Act at all. So my submission will be that the word 'reasonably', as in 'reasonably identifiable' in the definition of personal information, needs to be removed. That would also bring the definition of personal information closer into line with the GDPR and other laws around the world.

PHILLIPSON: I see this debate as the flipside of the coin to the definition of personal information. Somewhat echoing Anna's remarks above, there cannot be a gap between the two terms, but it is one of the reasons I

have such a hard time accepting that the definition of personal information should be expanded to encompass the situation where a person can be singled out vs actually be identified or reasonably identifiable.

This is because the definition of de-identified effectively becomes redundant. So long as a data set retains individualised characteristics, then we have the ability to re-identify the individual, even if it is just by singling them out.

I would retain the "reasonably identifiable" test, but in my opinion it needs to be linked to actual identification, not individuation. This solves one of the major issues that GDPR has caused – as the internet and digital services operate by delivering digital information to addresses, so that the content that is delivered to individual devices, nothing can be anonymous anymore. This was built out of the desire to protect against individuation, but has created quite a high compliance burden on digital participants that, in my opinion, is not necessarily justified. By returning to privacy for the individual, the role of de-identification and anonymization in providing true privacy risk mitigation is returned, and it also improves the ability to innovate using real-world, but de-identified, data sets.

FISHER: That's really interesting. Somewhat connected, could you explain the changes proposed to deal with inferred information?

JOHNSTON: The Discussion Paper proposes to add a definition of 'collection' that expressly covers inferred or generated information about people. This would put into statute what the OAIC has been saying for years, that the act of inferring information about people needs to be treated as a fresh 'collection', and the Collection privacy principles therefore need to be applied to that practice.

However we've already seen some pushback on this from Facebook. In their submission to the earlier Issues Paper, Facebook argued that the information it infers about people is very valuable to them, it's their intellectual property not our personal information, and they want to be able to use and monetise that data free from having to comply with privacy protections, which it describes as "inappropriate interference".

FISHER: Thank you, Anna. So an expanded notion of Personal Information increases the applicability of the Act. So too does the removal of existing exemptions. Looking now at them – small businesses, employee records, political parties – what's being proposed and is it the right approach?

FEHRENBACH: The Discussion Paper considers whether in light of some of the other proposals made there is a need to modify or remove the exemptions currently in the Privacy Act for employee records, registered political parties and small businesses. No particular proposal has been put forward, with the Paper noting that further consideration on those issues is required. For the most part, the Discussion Paper is seeking further input on some suggested options to amend those exemptions - not to remove them entirely.

On small businesses, currently most small businesses are not covered by the Privacy Act. A small business is one with an annual turnover of $3 million or less. The Discussion Paper notes that removal of this exemption could prove burdensome and indeed costly to small business owners. Instead, it canvasses a range of options including a reduction of the annual turnover threshold, limiting the scope of the exemption to some of the APPs, and requiring small businesses to comply with more basic rules or only in relation to high risk activities.

Australia does seem to be kind of out of step here – no equivalent jurisdiction exempts small businesses in the same way from its general privacy laws. Indeed, the Discussion Paper notes that in the 20 years since the exemption was put into place, technology has developed in leaps and bounds with even the more simplistic of businesses operating websites which easily capture large amounts of personal data. At the very least, modifying (if not removing) the small business exemption would create greater transparency with an aim of fostering an environment of trust with individuals who engage those small businesses.

In a similar vein, the Discussion Paper notes that removing the current employee exemption entirely would make it difficult to administer employee – employer relationships. At present, a private sector employer's handling of employee records in relation to current and former employment relationships is exempt from the Privacy Act, in certain circumstances. The Discussion Paper suggests that instead of removing this exemption entirely, a modification to allow better protection of employee records while retaining sufficient flexibility would be a more favourable amendment. Examples provided include introducing a standalone exception into APPs 3 (collection of personal information) and 6 (use and disclosure of personal information) in relation to the collection, use and disclosure of an employee's personal and sensitive information by a current or former employer for any act or practice directly related to the employment relationship. It is argued that this would allow for enhanced protection of employee privacy through the application of other APPs, for example APPs 8 (cross-border disclosure of personal information) and 11 (security/retention of personal information), whilst still allowing for the fundamental administration in an employment relationship.

This is a complex area in circumstances where for many, the risks to privacy have increased with the rise of working from home arrangements. This has led to a shift in boundaries between employees' personal and professional lives which the Discussion Paper notes make it more difficult to easily discern whether what aspects of an individual's personal information is protected or exempted under the Act. With those developments in mind, it seems an apt time for a modification to the current position to make this clearer.

Looking now to registered political parties, currently they are exempt entirely from the Privacy Act. A limited exemption applies for acts or practices done for any purpose in connection with an election, a referendum, the participation in another aspect of the political process or facilitating acts or practices of a registered political party by political representatives and their affiliates and by political parties' affiliates. The Discussion Paper is seeking further consideration and input on what impact there would be on the implied freedom of political communication and the operation of the electoral and political process if registered political parties were brought within scope of the more the limited exemption.

Requiring registered political parties to comply with the Privacy Act would bring Australia into line with the legislation across the pond in New Zealand. The Paper notes that some political parties in Australia already include privacy statements or policies on their website when they collect personal information, what information they collect and how they use it. Making this a requirement would at least, in my view, establish greater levels of transparency for how registered political parties deal with an individual's personal information, whilst not disturbing the implied freedom of political communication and the operation of the electoral and political process.

Overall, the Discussion Paper seems to be offering up a "if it ain't broke, don't remove it" position with respect to these exemptions, with a few tweaks here and there to bring them up to date with international legislation.

PHILLIPSON: From a privacy purist view, the small business exemption is an anachronism that I initially thought no longer had a place in a modern privacy regime when every business is a digital business. However, having spent some time considering the issue, I actually believe that there is a good argument for maintaining it, albeit with some modifications.

From my perspective, the key issue that should be focussed on is the risk of harm. It is right to state that a turnover threshold may no longer be appropriate if a small business is handling sensitive data of children, for example. So a proposal would be to create thresholds of data subjects and data types where, once exceeded or the data type is included, the exemption no longer applies. This would enable digital start-ups to innovate in a risk-based manner, with the risk of harm to individuals mitigated by either volume restrictions or not allowing sensitive or other high-risk data to be included.

If combined with limited application of some of the APPs across all personal information (for example APP 1 and 11), I think that such a regime would benefit Australia's digital ecosystem, balancing the private rights of individuals while promoting innovation. It would give Australian businesses access to the critical raw material (data) needed to develop new products and services whilst mitigating the overall societal risks. Further, it would not, in my opinion, be a barrier to international digital trade, as both the relevant laws of the exporting jurisdiction apply to such data and the relevant thresholds could be created such that it would be very rare that a small business would still be within them whilst expanding overseas in such a manner.

DAWSON: On the small business exemption, the presence of this exemption is one barrier to a GDPR adequacy decision being made in respect of Australia.

As Ashleigh noted, there are various reform options proposed in respect of the small business exemption, including:

- removing the small business exemption entirely;
- reducing the annual turnover threshold;
- replacing the annual turnover threshold with an employee number threshold;
- requiring small businesses to comply with some but not all of the APPs;
- developing simplified rules for small business;
- subjecting specific businesses, or specific acts and practices of small businesses that pose a higher risk to privacy and to the obligations set out in the Act irrespective of that business' annual turnover;
- providing small businesses with additional support; and/or
- introducing a voluntary domestic privacy certification scheme to allow small businesses that wish to differentiate themselves based on their privacy practices.

The lack of a GDPR adequacy decision impacts the decisions of EU-based companies to transfer to and/or store data in Australia, due to the additional compliance risks and costs, for example the requirement that a transfer impact assessment be undertaken. It also impacts Australia's ability to be a hub for data storage globally.

And on the employee records exemption, currently acts or practices involving the use and disclosure of personal information that directly relate to an employee record of a current or former employee are exempt from the Privacy Act, as Ashleigh touched upon. It is worth adding that in *Lee v Superior Wood* [2019] FWCFB 2946, the Fair Work Commission held that the exemption does not apply to collection of personal information. The discussion paper focuses on the application of the exemption to collection, with the following options being proposed:

- removing the employee records exemption entirely;
- modification of the exemption, for example by specifying that it only applies to APPs 3 and 6 (which govern collection, use and disclosure of personal information); or
- enhancing employee privacy protections in workplace relations legislation.

This is an important issue as regulators will need to balance employers' wishes to be able to manage employee information

without the constraints of the APPs against the implications of the exemption.

FISHER: One particular exemption that will be of interest to our readers is the Journalism exemption. Can you take us through it?

DAWSON: The journalism exemption is a critical provision of the Privacy Act. It is essential for the constitutional validity of the Act as it balances the right to privacy with the public interest in the free flow of information. As the Privacy Act currently stands, acts or practices carried out 'in the course of journalism' are exempt where the relevant organisation has publicly committed to deal with privacy by way of a public document.

Without the journalism exemption, media organisations would not be able to collect sensitive information without consent. Under the Privacy Act, 'sensitive information' includes philosophical and political beliefs. This could have a chilling effect on the freedom of political speech, for example where a politician privately expressed extremist views but refuses to consent to a journalist publishing such views.

As part of the Privacy Act review, the Attorney-General is considering:

- introducing a public interest test into the journalism exemption, so that it would only apply where journalism is, on balance, in the public interest;
- clarifying the definition of "journalism", for example by defining 'media organisation';
- specifying that APP 11 (which regulates information security and deletion/de-identification of personal information when it is no longer necessary) applies to media organisations; and/or
- strengthening the self-regulation model: by subjecting media and news organisations to a single standards scheme that would apply across different platforms, and would supported financially by digital platforms as distributors of news.

A key issue is whether to follow the broader journalism exemptions that apply overseas, for example under the GDPR, which reflect the need to embrace academic, artistic and literary expression.

FISHER: Let's shift our attention to individual rights, which also have a bit of a GDPR feel to them. Can you talk us through the right to object and portability?

FEHRENBACH: The Privacy Act does not currently include an equivalent right to 'data portability' or 'right to object' as we see in the GDPR throughout Articles 12, 20, 28 and 21.

In relation to data portability, the GDPR contains a right to receive data processed on the basis of contract or consent and processed by automated means, in a "structured, commonly used, and machine-readable format" and to transmit that data to another controller without hindrance.

Whilst the Privacy Act provides individuals with a right to request access to, and correction of, their personal information under APPs 12 and 13, the Act does not contain an equivalent portability right to the one we see in the GDPR. Interestingly, the Discussion Paper does not propose to introduce a general right of data portability under the Privacy Act, noting that doing so "may duplicate aspects of the Consumer Data Right (**CDR**), and create unnecessary complexity". The CDR so far has been implemented in the banking sector and provides data access/portability under a parallel regime to the Privacy Act. The energy and the telecommunications sectors will follow suit in time. On the basis that the CDR continues to expand across all industries over time, Australia may just have to wait a little longer for this individual right to apply.

Turning to another key individual right, under the GDPR the right to object

enables individuals to request that entities no longer process personal data in certain circumstances. It becomes available where personal data has been processed for the purpose of direct marketing, or for an entity's 'legitimate interests' or a 'public task' and the entity cannot demonstrate a 'compelling reason' to continue processing.

A key proposition of the Online Privacy Bill is to develop a code for online privacy organisations which may provide individuals the right to object to the further use or disclosure of their personal information. This would effectively allow individuals to stop or prevent others from processing their personal data, in certain circumstances.

A number of submissions highlighted the right to object under the GDPR and proposed that Australia should consider introducing something equivalent. The Discussion Paper proposes that an amendment to the Privacy Act be made such that an individual can object or withdraw their consent at any time to the collection, use or disclosure of their personal information. Upon receiving notice of an objection, an entity must take reasonable steps to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection. In doing so, this would greatly expand an individual's control and power over their personal information.

FISHER: Thanks Ash. An Australian version of the right to erasure has been proposed. How does it differ from its EU cousin, and how is it likely to affect a business?

GANOPOLSKY: Much will tun on the detail as to how the new right is drafted and incorporated into the broader sets of rights being considered in the reform process.

Just to recap, under Article 17 of the GDPR, data subjects have a right to obtain from certain entities ("controllers") the erasure of their personal data, without undue delay, where:

i. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; or

ii. the individual withdraws consent to use of their personal data; or

iii. the data subject objects to the processing of their personal data (subject to a certain procedure); or

iv. the personal data have been unlawfully processed; or

v. the personal data must be erased for compliance with a legal obligation in European Union law, or law of an EU Member State, to which the "controller" is subject; or

vi. the personal data have been collected in relation to certain services provided to a child.

In some cases, the right to process someone's data (by the entity) might override the individual's right to erasure. For example, where the data is being used to exercise the right of freedom of expression and information or is being used to comply with a legal ruling or obligation or is being used for the establishment of a legal defence or in the exercise of other legal claims. There are also exceptions for health related and public interest related purposes. For completeness, it is also important to note that in the EU, rights under Article 17 operate in the context of a developed body of law around the 'right to be forgotten' which is generally broader than the rights under Article 17.

As many readers will recall, the right was first articulated by the European Union Court of Justice in May 2014 in a case now known as the Google Spain case. The Court affirmed the existence of the right to have personal data deleted or de-referenced from search engines on request after a certain time upon fulfillment of certain conditions. For example, de-referencing of a link listed on a search engine when the page in question contains sensitive information such as information about religion, political opinion, or criminal conviction. This remains a developing area of the law in the EU, with some important differences as to how each supervisory authority applies the right in each context.

The 'right' being considered in section 15 of the Discussion Paper borrows from its 'cousin' but is different and potentially narrower than the rights applicable in the EU. I think these differences are important.

Regarding the scope of the information to be covered, the Australian principle will turn on what is 'personal information'. As Anna notes above, this definition is a key aspect of the pending reforms given that it impacts on the scope of the regime and its application to information rights of individuals, including erasure. It will be difficult, if not impossible, to give practical meaning to such a right in the absence of certainty as to what information is 'about' a person or 'relates' to a person.

The definition will, by necessity, impact on many technical and operational processes. APP entities will need to have robust processes in place to discern personal information from broader data sets. How each entity will address this will differ based on whether the entity operates a website, a communication service, or a social network. There may also be substantial variations based on industry practices. For example, in financial services there are prescribed requirements as to retention of customer data for regulatory purposes or in industries such a telecommunication, mandatory retention requirements on some types of personal information and meta data.

It will also be important to consider the right of erasure in light of important differences between the privacy regimes. In the EU, the right is to request and obtain the erasure 'from the controller'. Unless the 'controller' and 'processor' designations are introduced into the Privacy Act, the regime will need to address how the right will operate in the context of the supply chain and address the flow of information in the digital environment. It will be important to determine who has possession or control of the information in question. This raises issues as to who is deemed to be 'holding' the personal information and how responsibilities are addressed in the contract. Again, the industry involved, and type of information being processed, will be key as to how the right, as constituted, will apply in practice.

Lastly, we will need to be mindful that in the EU, the right of erasure arises in the context of human rights where privacy is a fundamental right, recognised in the European Convention for the Protection of Human Rights and Fundamental and Directive 95/46. There is no such corresponding right in Australia and the Discussion Paper does not propose to change this. I think this will have a direct bearing on how the right is understood and administered.

FISHER: Thanks Olga. There's a recommendation to create a direct right of action, and a separate recommendation to introduce a statutory right for invasion of privacy. To our private practice lawyers, would you say that you're licking your lips all the time these days or just constantly? Seriously, though, can you talk us through these proposals and how they will differ?

DAWSON: The direct right of action, if introduced, is set to cover 'interferences with privacy' by an APP entity (i.e. only those entities subject to the Privacy Act). Such complaints will be subject to a 'conciliation gateway' similar to claims brought under discrimination legislation, whereby the claimant would first need to make a complaint to the OAIC and have their complaint assessed for conciliation. The complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or where the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court for it to be heard by the Federal Court or Federal Circuit Court.

By contrast, if a statutory tort were introduced, a claimant would have the choice to bring an action (against any entity liable to be sued in Australia, not just APP entities) directly in Court under either of two limbs:

- intrusion upon seclusion (usually involving intrusions into a person's physical private space, such as watching, listening to and recording another person's private activities, as opposed to information privacy, as regulated by the Privacy Act); or
- misuse of private information (which is defined by the ALRC to constitute unauthorised disclosure). While this may constitute an 'interference with privacy', as under the proposed direct right of action, interference is likely to be construed to be broader, to include various other interferences (such as poor security or collection practices). Also unlike under the proposed direct right of action, such a tort would also not likely be tied to the definition of personal information nor subject to the exemptions in the Privacy Act.

The statutory tort being contemplated would also require proof of the following elements:

- that the public interest in privacy outweighed any countervailing public interest;
- that the breach of privacy satisfied a seriousness threshold; and
- that the complainant had a reasonable expectation of privacy in all the circumstances.

GANOPOLSKY: I think the fact that the other common law jurisdictions have developed the tort and the post GDPR developments, mean that Australia is now out of step. Having a statutory tort will mean that the legislature will have a say in framing the right and can address the scope of the right in light of current circumstances and priorities.

FISHER: A great deal of focus in the Discussion Paper is on the way the law is enforced. The Privacy Commissioner is likely to receive some expanded powers, and the penalties are going to increase significantly. The Privacy Commissioner has traditionally been a more educative and collaborative regulator than a penaliser. But this may change. How important is this development?

JOHNSTON: I would love to think that all organisations care about the privacy of their customers and staff because they know it's a matter of trust and reputation, but there's nothing quite like the prospect of large fines to gain the attention of the C-suite and move privacy compliance up the 'to do' list!

In recent years the OAIC has done a remarkable job with the limited resources it has. It's been quite strategic in its choice of investigations into large companies and government agencies, and in the use of its Determination power. But to be an effective regulator with reach across the entire economy, it needs a full range of tools in its regulatory and enforcement toolkit. The proposals in the Discussion Paper, and in Schedules 2 and 3 of the Online Privacy Bill, are about finally giving the OAIC that full toolkit. But they will also need a significant funding boost to go with it.

FISHER: ...which brings us now to the Online Privacy Bill. Can you summarise its purpose and effect?

JOHNSTON: Schedule 1 of the Online Privacy Bill is about creating a space in the Privacy Act for the introduction of a binding 'Online Privacy Code'. The Code would create new obligations for certain kinds of bodies, namely social media companies, data brokers, and large online platforms, as Ashleigh mentioned earlier. Either the industry would need to develop the Code within 12 months, or the OAIC can step in and develop it.

The content of the Code would need to flesh out how some of the APPs will apply in practice to those industries, and would cover three broad areas: how to draft privacy policies and collection notices and what consent means; introducing a right to object, which means the ability for a consumer to ask a company to cease using or disclosing their personal information; and some requirements to protect children and other vulnerable groups.

The Discussion Paper for the main review process says that the Online Privacy Bill "addresses the unique and pressing privacy challenges posed by social media and online platforms". But in reality most of those issues, and the proposed solutions, like the role of notice and consent and how to protect children, are not unique to social media or online platforms, and in fact all but one of the issues proposed for the Code are already addressed in the broader Discussion Paper.

The one big thing that's proposed for the Code that's not also in the Discussion Paper is age verification for the use of social media, along with a requirement for parental consent to sign up users under 16. This means age verification for everyone, not just children. And age verification usually means identity verification, which means giving Big Tech *more* personal information, which in my view is not very privacy-friendly, for a Bill supposed to be about privacy.

SAINTY: From a practical point of view the Online Privacy Code, as described in the Bill, is an ambitious exercise.

It is a part of the Government's response to the Digital Platforms Inquiry which recommended enhanced privacy protections for individuals online. As Anna rightly points out the Online Privacy Code is to be developed and registered within 12 months. The relevant organisations to be governed by the Code (**Code Participants**) will have the first opportunity to do this – at the request of the Information Commissioner. However, if the Code is not suitable, the Commissioner may develop it herself. On that basis, it's hard to see an agreed Code in circulation within 12 months.

One challenge, besides the time frame, is that the Code Participants are likely to have many and varied views on the approach to and impact of such a Code. There is no current uniform view on the topics the Online Code is to cover – policies, collection notices and consents (including a right to object) – and very different vested interests among the Code Participants. The Code Participants themselves are not a clearly defined class.

FISHER: The Exposure Draft of the Bill and an accompanying Explanatory Paper were released at the same time as the Discussion Paper for the broader review of the Privacy Act. What are your thoughts about the timing? Why are these two related pieces of privacy law reform separate, and what are the risks and benefits with that approach?

DAWSON: Our discussions with the Attorney-General indicate that the reforms set out in the Code are likely to be passed in early 2022, with the broader reform to the Privacy Act occurring in late 2022, likely to come into effect at some point in 2023.

JOHNSTON: Politically, the government is keen to be seen to beat up on Big Tech ahead of the election. This is driven by reactive politics rather than sensible policy. That's my summary of the two strands: one is policy, the other is politics.

My concern is that the debate over age verification will prove to be a furphy which distracts from the bigger issues raised by the wider Act review. The Government should fix the Privacy Act for all regulated entities and all Australians, instead of introducing a two-tier regulatory system. Any new provisions for protecting children and vulnerable groups, or for clarifying the elements needed to gain a valid consent, should apply to all sectors, as is already proposed in the Discussion Paper as part of the broader review of the Privacy Act.

Plus, being pragmatic, in my view, none of the proposals for the Online Privacy Code will be effective at protecting privacy in practice until the definition of 'personal information' is first fixed, as is proposed in the Discussion Paper, but not included in the Bill.

FISHER: How will the Online Privacy Code impact on children's privacy?

LINDHOUT: Many people including parents like myself will be excited to see that the Online Privacy Code seeks to increase the protections available for children and vulnerable groups. I touched on increased protections for children in the general privacy law reform process; but this process is focused on social media providers, data brokers and large online platforms, where there is a special need for child protection. Presently, privacy protection for children is not something directly addressed in the Privacy Act, only in guidance from the OAIC. So the first step is to formalise protection for children in the Code rather than just guidance materials.

But more substantively, it is proposed that the Code will have two layers of privacy obligations: (a) the first for all Code Participants; and (b) a second layer of additional obligations for social media platforms. For all Code Participants, it's proposed that the Code will set out how various privacy obligations will apply specifically in relation to children. For example, there might need to be a children-specific privacy policy and collection notice. There would be greater clarity on the collection, use and disclosure obligations in relation to children's personal information. The point here is that if Code Participants are forced to set out specifically how they deal with children's personal information, there will be greater protection in turn.

The second layer of protection that is proposed to apply only in relation to social media platforms involves a stricter set of obligations for handling children's personal information, namely that social media service providers will need to:

- take all reasonable steps to verify the age of individuals who use the service;
- ensure that the collection, use and disclosure of a child's personal information is fair and reasonable in the circumstances, with the best interests of the child being the primary consideration when determining what is fair and reasonable; and
- obtain parental or guardian consent before collecting, using or disclosing the personal information of a child who is under the age of 16, and take all reasonable steps to verify the consent.

The stricter standard to be applied to social media service providers arises expressly because, as the Explanatory Paper puts it, the potential risks social media platforms pose to children are higher than those posed by data brokers or large online platforms due to: (a) the number of children who use social media services; (b) the nature of the interactions that can occur via social media platforms; and (c) the wide range and volume of personal information that social media platforms handle.

The next challenge will be addressing in the Code how you determine what reasonable steps are in the context of a social media platform assessing whether parental consent has actually been obtained. Given the very nature of online interactions which the Code is seeking to make safer, it's likely this will be a tricky one to bed down.

FISHER: Thanks Beck. So what are next steps in the privacy law reform process?

FEHRENBACH: On 6 December 2021, the Government closed submissions on the Online Privacy Bill and consultation Regulation Impact Statement. We are now waiting in anticipation for further developments on the Online Safety Bill before it is introduced to Parliament.

The government is inviting submissions and any feedback on the proposals in the Discussion Paper until 10 January 2022. This will inform the Privacy Act Review's final report. The Attorney General's website advises that Privacy Act Review seeks to build on the outcomes of the Online Privacy Bill "to ensure that Australia's privacy law framework empowers consumers, protects their data and best serves the whole of the Australian economy".

I don't need a crystal ball to tell you that 2022 will be another big year for developments in privacy in Australia.