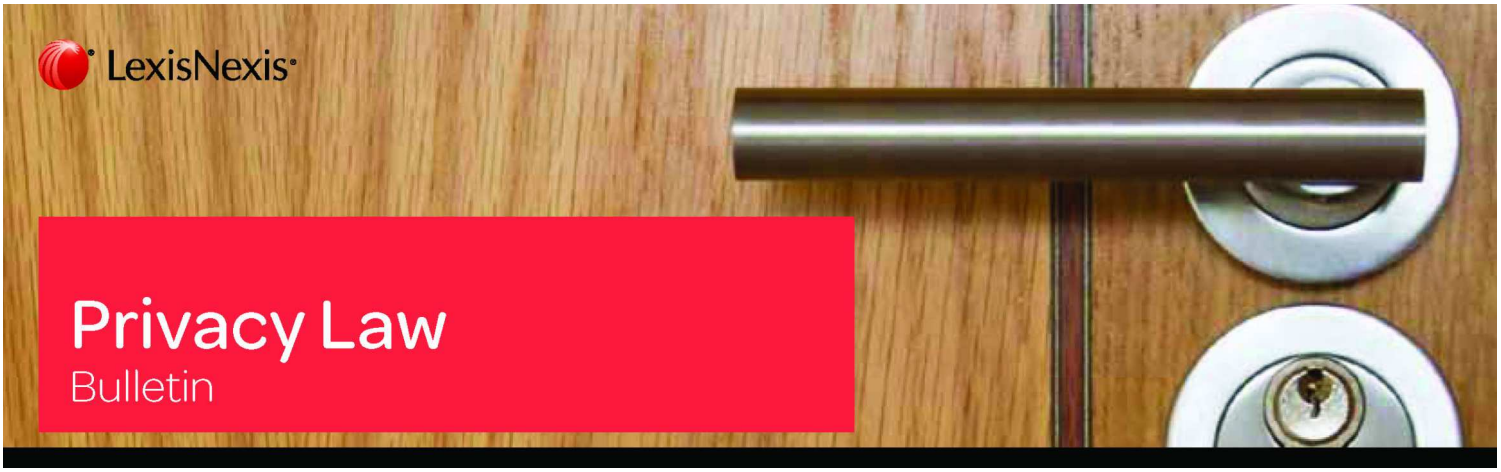

Privacy Law Bulletin

2021 . Vol 17 No 9

Contents

Information contained in this newsletter is current as at February 2021

LexisNexis® Butterworths

Interview with Anna Johnston, Principal of Salinger Privacy

Sharon Givoni *SHARON GIVONI CONSULTING*

What did you do before you started your own privacy consultancy in 2004?

Immediately before starting Salinger Privacy I worked as the Deputy Privacy Commissioner for NSW. Before that I worked in a variety of legal, policy and research roles, mostly in the public sector, but also a brief stint in private practice. I got into privacy when I was the principal legal officer for a NSW government department and we were helping to implement the NSW privacy laws when they were new back in 1998.

What sort of privacy work do you cover in your practice?

We provide privacy advice to clients from ASX [Australian Securities Exchange] top 10 companies to start-ups, NGOs and public sector agencies. One of our particular strengths is being able to translate privacy law for new audiences, and develop pragmatic solutions for our clients, whether they need a review of a new technology, help designing a framework for making decisions about ethical data use, or maybe drafting plain language comms for their customers.

That issue of data use and data sharing is a common one; we have a number of clients doing really interesting work in data analytics in public interest areas like medical research, or informing public policy on how best to protect children or educate students or support vulnerable populations. Being able to achieve those objectives depends so much on public trust and gaining a social licence, so getting their privacy settings right is a really critical issue for them. It's a real privilege to work with so many clients who intuitively know that they have to get privacy right, and we love to add value by helping them achieve their objectives.

When did you know that you wanted to do privacy law exclusively and what is it you enjoy about this area of law?

I was hooked on privacy as the lens through which to think about technology, ethics and the law from pretty much the day I started work as the Deputy Privacy Commissioner. That was so long ago now, before September 11 and the explosion in government surveillance capabilities that that precipitated, and before social media and smartphones and AI and the Internet of Things and all the privacy challenges that have come with those technological developments.

What I love about working in the privacy space is that there's always something new. So in any given week we might be developing some customised Privacy by Design training for a client, giving advice on how to implement data governance in a meaningful way, perhaps working on a Privacy Impact Assessment of some interesting new technology project, maybe a chatbot, or the establishment of a data analytics project. But no matter what kinds of projects we are looking at, the basic questions are the same: can and should we collect this data, can and should we use it for this purpose, to whom can we disclose it and how do we keep it safe?

What do you see as the greatest challenge for future privacy lawyers?

Whether lawyers or not, privacy advisers need to stay abreast of the legislative landscape as well as emerging technologies, and shifts in community attitudes. Being a good privacy advisor means understanding not just the law, but how to help clients integrate privacy into their business.

The law can only ever achieve so much on its own. It's so much better to factor privacy controls into the design of systems from the beginning. When a client is designing, configuring or implementing tech, you also have to think about the authorised users of that system, and design the tech so that authorised users only see the minimum amount of personal information they need to do their job.

Privacy controls can be built into tech, whether that is filtering out certain data fields from entering a data warehouse, setting role-based access controls on a CRM [customer relationship management], masking certain data fields from view of certain users, requiring users to pass tests or offer assurances before they can access data, audit trails and proactive monitoring of them,

just-in-time collection notices or permission requests . . . there's plenty you can do. We use eight privacy design strategies to guide our advice to clients when we do Privacy Impact Assessments.

Do you think that the current privacy laws are threatening or hindering the progression of new technologies?

Mostly I see privacy laws as an enabler of good, fair technologies, rather than as a barrier. You need privacy laws to create a safe space in which to innovate. There is some interesting research from the UK which found that the sectors which were most highly regulated in terms of privacy actually were the most advanced in the adoption of AI.

And, in fact, where we have weaknesses or gaps in our privacy laws, fixing them and strengthening privacy laws can help spur more growth and innovation. The recently-announced review of the Privacy Act 1988 (Cth) will be examining how our law can be beefed up, so that Australia can be recognised as "adequate" by the European Union. An "adequacy" decision would open doors for Australian businesses trying to reach European markets, because then personal information could be exchanged freely. And, I might add, New Zealand, which from 1 December in 2020 placed restrictions on sending personal information to Australia unless our law is considered to match New Zealand's standards. At the moment, we fall short in Europe's eyes, because of a number of exemptions which other countries' privacy laws do without: exemptions for small businesses, employee records, media organisations and political parties. New Zealand might take the same view; that's yet to be determined. But if they do, then Australian businesses will need to jump through more hoops to be able to work with organisations in New Zealand, and that may pose a competitive disadvantage if they are competing against companies operating in New Zealand or Europe or other "adequate" jurisdictions.

In your view, is it possible to enact technology-neutral legislation?

Absolutely. Privacy law is a good example of that. Lack of enforcement, perhaps lack of understanding or even awareness of the privacy principles are all problematic, but in terms of the foundational principles, they are intended to apply in a technology-neutral way, and for the most part I think they succeed.

Statute law needs to be adaptive. The "fuzzy" nature of privacy law is one of the things I love about it — you do need to use your judgment, and think about what your customers would expect, and what you can do to avoid causing them any harm. The interpretation of what is "reasonable" is shifting all the time, and that's a good thing. It's how privacy law manages to stay relevant to both new technologies and shifts in community expectations. If the law was more prescriptive it would quickly become out of date.

If you could change one thing in privacy law what would it be?

There is one thing that I am super passionate about, and that is individuation. So if I had a magic wand and could fix one thing about privacy law, I would make sure that the threshold definition of "personal information" or "personal data", in privacy laws around the world, incorporated not only individuals who are *identifiable*, but also who can be *individuated* to a degree that facilitates their tracking, profiling or targeting.

Too much activity is currently escaping regulatory scrutiny because companies can conduct really intrusive online tracking and targeting. This has really significant effects not only on privacy but social cohesion and the maintenance of public trust in our democratic institutions. The companies responsible are saying "oh but it's not personal information because we don't know the real identity of these people we're targeting, so we don't need to comply with the privacy laws".

Is de-identifying personal data enough to protect privacy?

No. It can be useful as a risk mitigation strategy, but re-identification risk is constantly growing. As I mentioned before, individuals can be singled out for profiling and targeting online even if their identity cannot be known. The focus of privacy law needs to shift towards preventing privacy harms. Being "not identifiable" is no longer a suitable proxy for "not suffering privacy harm".

Data security is a hot topic. How does it differ from privacy law?

Data security is just one aspect of privacy law and practice. Within the umbrella of data security sits the management of information security and cybersecurity which is the domain of the chief information security officer, but it also encompasses having other strategies and controls including building robust data governance, policies and procedures, staff training around appropriate personal information handling practices, data minimisation strategies, etc — all of which sits with the chief privacy officer.

Do you believe that Australia should introduce a tort of privacy?

Yes. It is necessary to help address harms arising from serious invasions of privacy which are not already regulated by enforceable privacy principles. But a tort is

not enough, we also need financially accessible justice such as a direct right of action to enforce compliance with privacy principles under the federal Privacy Act, in a relatively cheap tribunal, the way we have under NSW privacy law. The Privacy and Personal Information Protection Act 1998 (NSW) allows complainants to seek an internal review from a respondent agency, and then they have a right to apply to the NSW Civil and Administrative Tribunal (NCAT) for external review.

Do you believe that Australia has a different approach to privacy law from the UK and the US? Explain.

Australia is closer to the UK's approach than the US, that's for sure, although we do not have an enforceable charter of human rights like the UK and Europe do.

The US is the outlier when it comes to privacy law, because it lacks an omnibus approach; omnibus privacy laws cover all sorts of organisations, not just one sector of the economy. While the newish Californian law, the California Consumer Privacy Act (or CCPA), takes an omnibus approach, it is so deeply flawed that if anything, in my view, it just entrenches the very kind of surveillance capitalism behaviour it is supposed to stop.

The US model of privacy regulation is to rely on their consumer laws, and I think that this has utterly failed as a regulatory model. It elevates notice or transparency as a privacy control, way above its real value. The US model says, "so long as we *tell* you how we're going to abuse your privacy we're complying with the law", and then says that because they were given notice, consumers are "consenting" to what businesses are doing with their data. That's just absurd, a legal fiction which is hopefully on its deathbed.

That practice of dressing up notice as "consent", when we all know it's not valid from the individual's point of view, that drives me nuts. If it's a collection notice or buried in a privacy policy, it's not consent. If it's a condition of doing business with you, it's not consent. If I had no genuine choice to say "no", it's not consent. I describe consent as the "would you like fries with that?" question. If I can freely say no to the fries, but still get the burger I want, without any kind of penalty for saying no to the fries, then if I do say "yes" to the fries you can call it consent. But let's not pretend that anyone using Facebook, or any other digital platform or service really understands, let alone consents to, all the myriad ways in which that company is going to use their personal information.

The ACCC's [Australian Competition and Consumer Commission] *Digital Platforms Inquiry* perfectly captured the interplay between data collection as the business model driving big tech, and the impacts that it has on us as consumers and as citizens, both from a privacy perspective and from an economic perspective, in terms of Google and Facebook in particular having effective monopolies. Their market worth is entirely based on exploiting our personal information.

So whether you are talking Australia, the UK or the US, the way forward has to involve an understanding of the role to be played by both privacy and consumer protection/trade practices law and regulators.

Do you think that privacy is a subject that should be taught to all law students at law school today?

I would love to see it as an elective subject in all law schools at least. It didn't exist at all as a subject when I was in law school, but privacy and data protection have become so central to how we live and how almost every business operates that lawyers should at least know the basics.

But I wouldn't want it taught as just some tick-a-box compliance exercise. It's easy to get caught up in the minutiae of APP this and exemption that, but mostly privacy law boils down to common sense and good manners. And increasingly you need an appreciation for community attitudes towards privacy, which are always shifting. My advice for lawyers is to be less lawyerly; take a step back and look at the bigger picture. Because the law might say whether your client "can", but not whether they "should".

Photo of Anna Johnston

Salinger Privacy was established in 2004 and offers a range of privacy resources including template policies and procedures, eLearning and face-to-face compliance training options, and privacy consulting services. It is on the Australian Government's Privacy Services Provider Panel for Privacy Impact Assessments, privacy advice, and privacy training; is a fully pre-qualified

supplier to the NSW Government; under the NSW Prequalification Scheme and is an approved supplier on the Victorian Government's eServices Register and the Australian Government's Digital Marketplace in relation to our privacy resources and privacy training solutions.

Sharon Givoni
Principal Lawyer
Sharon Givoni Consulting
sharon@iplegal.com.au
www.sharongivoni.com.au

Privacy Law
Bulletin

Disclosing genetic information to family members without consent in Australia

Jane Tiller, Gemma Bilkey, Rebecca Macintosh, Sarah O'Sullivan, Stephanie Groube, Marili Palover, Nicholas Pachter, Mark Rothstein, Paul Lacaze *and* ***Margaret Otlowski***

Introduction

Genetic variants that increase risk for disease are hereditary, meaning genetic risk information is relevant for individuals and their blood relatives. Health practitioners (HPs) routinely advise patients with such genetic variants of the disease risks faced by their family members and the importance of sharing genetic results with at-risk relatives. This is especially important for clinically actionable pathogenic variants that increase risk of preventable conditions, such as *BRCA1/2* variants, where surveillance and/or risk-reducing surgery can be life-saving.[1] However, some patients choose not to share genetic results, or do not consent to HPs sharing results with their blood relatives.[2] In such circumstances, HPs must choose whether to disclose genetic information to relatives without consent. This requires an understanding of their legal and ethical obligations and what discretion is available to them, which research shows many HPs lack.[3] HPs may be reluctant to discuss such issues when they arise for fear of legal ramifications, and until recently there have been few (if any) published case studies regarding these issues. Here we expand on recent commentary[4] to provide an up-to-date and clinically accessible resource for HPs with access to genetic information. This paper is adapted from our recent publication[5] which also considers five clinical case studies that have arisen in Australian public genetics services and the application of these laws, guidelines and principles to real-life scenarios.

International approaches

International approaches to non-disclosure without consent vary.[6] A recent UK case[7] examined whether HPs in the UK have a positive legal duty to advise family members of their genetic risk, even without patient consent. A woman (ABC) sued her father's HPs for not disclosing that he had the genetic variant causing Huntington disease, a progressive and incurable neurodegenerative disorder. Her father's HPs had advised him of ABC's 50% risk of inheriting the variant, but he refused to consent to disclosure to her. Consistent with recent suggestions of introducing a "duty to consider" in the UK[8] the court found that where a proximate relationship exists between a patient's HP and an at-risk relative, the HP has a duty of care to conduct a balancing exercise as to the benefit to the relative of being informed of the genetic risk and the patient's interest in maintaining confidentiality. If the balancing exercise favours disclosure, there is a duty to disclose. If a balancing exercise has been properly conducted, and a conclusion that disclosure should not be made is reasonably reached, the HP's duty will be fulfilled. ABC was unsuccessful at trial, as the court found that the relevant HPs' decision did not breach the applicable duty.[9]

Other approaches vary by country. In France, for example, patients who learn of genetic risks are legally required to inform their at-risk relatives of their possible risk — either directly or by providing consent to their HP to contact relatives for this purpose.[10] Research indicates that in practice, disclosure by patients is the preferred course and HP disclosure may be rare.[11] In the US, a single state court case held that HPs have a duty to warn a patient's relatives of genetic risks.[12] However, this was overruled by subsequent federal health privacy legislation which prohibits any disclosure of health information to relatives by a HP without consent.[13]

Australian position

In Australia, disclosure of genetic information by a health practitioner without consent has legal and ethical aspects. Various state and federal statutory privacy regimes, designed to protect the privacy of personal information, prohibit the use or disclosure of personal information without consent except in specific circumstances.[14] Further, HPs owe a common law (non-statutory) duty of confidentiality to patients whose confidential information they hold.[15] If a HP discloses genetic information without consent, this is a potential breach of both statutory privacy obligations as well as the common law duty of confidentiality. There is currently no established Australian legal duty to disclose genetic information to a patient's at-risk relatives, but there are some laws and guidelines governing use/disclosure of genetic information that can be relied on

by HPs. However, these are inconsistent and information about how often HPs rely on them is lacking.[16]

McWhirter et al recently discussed the legal and ethical issues surrounding unconsented disclosure of genetic results to relatives in Australia and the discretion available to health practitioners.[17] The discretion available to HPs in Australia varies by state, as well as by the context in which the practitioner works (public/private).[18] Under s 16B of the Privacy Act 1988 (Cth), which applies to HPs in the private health system, use/disclosure of genetic information by HPs without consent is allowed as an exception to the applicable privacy obligations. However, the exception only applies where there is a *reasonable belief that disclosure is necessary to lessen or prevent a serious threat to life, health or safety of a genetic relative*. The exception is accompanied by National Health and Medical Research Council (NHMRC) guidelines[19] which must be followed if a HP decides to use/disclose the private information.

Notably, the protections provided to HPs that choose to exercise the discretion to disclose genetic information about a patient to a genetic relative relate directly to any potential breach of the Privacy Act rather than potential liability for breach of confidentiality. Here we focus on the implications for liability regarding statutory breach of privacy, however we note that the framing of the guidelines minimises the risk of breach of confidentiality if followed. In particular, guideline 7 requires that disclosure be limited to genetic information necessary for communicating the risk, and where possible avoids identifying the patient or conveying their lack of consent for disclosure.

As discussed, the Privacy Act and NHMRC guidelines apply to private health providers, but not to public health providers, which are governed by the laws of their state or territory health system. New South Wales (NSW) has enacted legislation very similar to the Federal regulations, which applies to all public health providers.[20] Further, NSW has adopted the relevant portions of the NHMRC guidelines, meaning that those guidelines also apply to public HPs in NSW. All other states/territories have a legislative scheme with some allowance for unconsented use/disclosure of personal information,[21] although not all necessarily apply to genetic information, as discussed below. None but NSW have duplicated the NHMRC guidelines or developed jurisdiction-specific guidelines. In Tasmania, however, guidelines have been developed which endorse the use of the NHMRC guidelines by Tasmanian HPs, and provide interpretation of the guidelines in the context of the Tasmanian statute.[22]

Significantly for Victorian HPs, the Victorian legislative framework has changed in recent years. Previously, the discretion to disclose private health information without consent only applied where risk to an individual was both serious *and* imminent, meaning predictive genetic risk disclosure would rarely, if ever, be covered by the exception.[23] This position has been altered by recent legislative changes (unrelated to the specific issue of genetic disclosure), which have removed the word "imminent".[24] This means risk must now only be serious[25] for the discretion to apply. This brings the Victorian position into line with the federal and most other state/territory positions, and means that, it does arguably now apply to genetic information. However, the Northern Territory (NT) and Australian Capital Territory (ACT) have not updated their legislation, retaining the requirement that risk be imminent before disclosure without consent can take place. *This means that HPs working in public health services in the NT and ACT are arguably unable to rely on this discretion to disclose genetic information to at-risk relatives without consent*. The laws which were passed more recently do not contain the requirement that risk be imminent for disclosure to be permissible. Given the public health inequities created by this inconsistency, Territory governments should now consider updating their legislation to align with the more recent federal and other state positions, ensuring that the discretion to disclose information would extend to genetic information.

It is important to note that there is no absolute duty to disclose genetic information to a relative without consent in any circumstances in Australia. In some cases, HPs will decide not to disclose information even when the discretion is available to them. The reasons for this will vary but may include concerns about family relationships, working with the patient to keep trying to encourage personal disclosure, or other individual considerations. In some circumstances, waiting too long to disclose may result in serious harm — for example, the development of preventable cancer in a patient with a breast cancer gene (BRCA) variant. However, in some cases, the passage of time removes the need to disclose. In each case, the HP must consult with colleagues and consider not only whether disclosure is necessary, but also whether to wait, and what period of time is appropriate before the decision to disclose is made. The NHMRC guidelines contain guidance regarding these considerations in various scenarios.

Even in jurisdictions where these guidelines have not been explicitly adopted, they can provide a framework for HPs considering their exercise of discretion. The NHMRC guidelines are only applicable to HPs who are considering disclosing a patient's genetic information to genetic relatives. They do not apply to other professionals, entities or members of the public who hold genetic information, or to the disclosure of information to third parties who are not genetic relatives. Further, they do not

cover every scenario that could arise — for example, the guidelines explicitly state that they are not applicable to situations concerning genetic information that present a serious threat to an unborn child. However, they are the most robust form of guidance available for Australian HPs considering how to exercise their discretion. Although the guidelines do not explicitly apply to public health services in states or territories outside NSW, Tasmania's approach in endorsing the use of the guidelines by HPs considering an exercise of discretion to disclose without consent is sensible. Considering and agreeing how the guidelines apply to state-specific legislation and endorsing following of the guidelines in exercising discretion in each state would provide harmonisation, reduce confusion and inequity, and promote access to a clear, consistent framework for Australian HPs.[26] The authors are not aware of any current discussions at the Australian policy level in this regard, but our recent publication[27] highlights the importance of this issue.

Conclusion

In Australia, there is currently no established legal duty to disclose genetic information to a patient's at-risk relatives, and privacy laws and the common law duty of confidentiality prohibit disclosure without consent in most circumstances. However, there are laws and guidelines which provide exceptions to the statutory privacy obligations and allow for unconsented use/disclosure of genetic information without breaching privacy law. These protections do not extend to obligations of confidentiality, but the guidelines which have been developed at a federal level minimise the risk of breaching confidentiality obligations. Many HPs do not understand their obligations in considering these issues. Here we have discussed the differing regulations which apply to Australian HPs in different health service contexts, to provide some practical guidance to HPs faced with such decisions.

Notwithstanding jurisdictional variations in law and policy, it is important that all HPs follow a clear decision-making process when considering the exercise of this discretion. The NHMRC guidelines provide guidance regarding the exercise of this discretion, which can be helpful even where they have not specifically been adopted. Adopting these guidelines nationally would assist with much-needed national harmonisation in this area. International policy makers grappling with how to balance the right to genetic risk information with duties of confidentiality may also benefit from considering these guidelines and their local applicability.

The authors declare no conflicts of interest. No financial assistance was received in support of the study.

Author team

Jane Tiller
BSc/LLB(Hons); MGenCouns
Public Health Genomics, Monash University, Melbourne Australia
jane.tiller@monash.edu

Gemma Bilkey
MBBS(Hons); MPH
Western Australian Department of Health, Perth, Australia

Rebecca Macintosh
MGenCouns
Centre for Clinical Genetics, Sydney Children's Hospitals Network

Sarah O'Sullivan
BSc(Hons); Grad Dip GC

Stephanie Groube
MGenCouns
Tasmanian Clinical Genetics Service

Marili Palover
MSc
Institute of Genomics, University of Tartu

Nicholas Pachter
MBChB; FRACP
Genetic Services of Western Australia

Mark Rothstein
JD, University of Louisville School of Medicine

Paul Lacaze
BSc; PhD
Public Health Genomics, Monash University, Melbourne, Australia

Margaret Otlowski
LLB(Hons); PhD
University of Tasmania

Table 1: Summary of legislation and guidelines applicable to health practitioners in Australian jurisdictions

Jurisdiction	Legislation	Application of discretion	Provision	Guidelines available for use by practitioners to guide discretion?
Federal (Cth)	Privacy Act 1988	Available to HPs working in private health settings — must follow guidelines.	**Section 16B(4) — Use or disclosure — genetic information** A ***permitted health situation*** exists in relation to the use or disclosure by an organisation of genetic information about an individual (the ***first individual***) if: (a) the organisation has obtained the information in the course of providing a health service to the first individual; and (b) the organisation reasonably believes that the ***use*** *or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the first individual*; and (c) the use or disclosure is conducted in accordance with guidelines approved under section 95AA; and (d) in the case of disclosure — the recipient of the information is a genetic relative of the first individual. (Emphasis added.) **Section 95AA — Approving guidelines for use and disclosure** (2) For the purposes of para 16B(4)(c), the Commissioner may, by legislative instrument, approve guidelines that relate to the use and disclosure of genetic information for the purposes of lessening or preventing a serious threat to the life, health or safety of an individual who is a genetic relative of the individual to whom the genetic information relates.	Yes *Use and disclosure of genetic information to a patient's genetic relatives under s 95AA of the Privacy Act. Guidelines for health practitioners in the private sector*. National Health and Medical Research Council (NHMRC) (2014).

Australian Capital Territory (ACT)	Health Records (Privacy and Access) Act 1997	Arguably does not allow for disclosure of genetic info as risk must be imminent.	**Schedule 1 —The Privacy Principles** **Principle 9: Limits on the *use* of personal health information** 1 Except where personal health information is being shared between members of a treating team to the extent necessary to improve or maintain the consumer's health or to manage a disability of the consumer, a record keeper who has possession or control of a health record that was obtained for a particular purpose must not use the information for any other purpose unless— . . . b) the record keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a significant risk to the life or physical, mental or emotional health of the consumer or another person . . . **Principle 10: Limits on *disclosure* of personal health information** 1 A record keeper who has possession or control of a health record must not disclose personal health information about a consumer from the record to an entity other than the consumer. 2 Clause 1 does not apply to the disclosure of personal health information about a consumer to an entity if — . . . (d) the record keeper believes, on reasonable grounds, that the disclosure is necessary to prevent or lessen a serious and imminent risk to the life or physical, mental or emotional health of the consumer or someone else . . . (Emphasis added)	No

New South Wales (NSW)	Health Records and Information Privacy Act 2002	Available to HPs working in the NSW public health setting — must follow guidelines.	**Schedule 1 Health Privacy Principles** **10 Limits on use of health information** 1) An organisation that holds health information must not *use* the information for a purpose (a ***secondary purpose***) other than the purpose (the ***primary purpose***) for which it was collected unless — . . . (c1) **Genetic information** the information is genetic information and the use of the information for the secondary purpose— (i) is reasonably believed by the organisation to be ***necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of a genetic relative*** of the individual to whom the genetic information relates, and (ii) is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph **11 Limits on disclosure of health information** 1) An organisation that holds health information must not *disclose* the information for a purpose (a ***secondary purpose***) other than the purpose (the primary purpose) for which it was collected unless— (cl) **Genetic information** the information is genetic information and the disclosure of the information for the secondary purpose— (i) is to a genetic relative of the individual to whom the genetic information relates, and (ii) is reasonably believed by the organisation to be necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of a genetic relative of the individual to whom the genetic information relates, and	Yes *Use and disclosure of genetic information to a patient's genetic relatives: Guidelines for organisations in NSW*. New South Wales Information and Privacy Commission (2014). [mirrors relevant sections of Federal NHMRC guidelines]

			(iii) is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph.	
Northern Territory (NT)	Information Act 2002	Arguably does not allow for disclosure of genetic info as risk must be imminent	**Schedule 2 Information Privacy Principles** **IPP 2 Use and disclosure** 2.1 A public sector organisation must not use or disclose personal information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose for collecting it unless one or more of the following apply: . . . (d) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent: (i) ***a serious and imminent threat to the individual's or another individual's life, health or safety*** (Emphasis added.)	No
Queensland (Qld)	Information Privacy Act 2009	Available to HPs working in the Qld public health setting	**Schedule 4 National Privacy Principles** **NPP 2 — Limits on use or disclosure of personal information** 1) A health agency must not use or disclose personal information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose of collection unless — . . . (d) the health agency reasonably believes that the use or disclosure is ***necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare*** or a serious threat to public health, safety or welfare. (Emphasis added.)	No
South Australia (SA)	Health Care Act 2008	Available to HPs working in the SA public health setting.	**Section 93 — Confidentiality** (3) Subsection 2 does not prevent a person from — . . .	No

			(e) disclosing information if the disclosure is ***reasonably required to lessen or prevent a serious threat to the life, health or safety of a person***, or a serious threat to public health or safety (Emphasis added.)	
	PC012 — Information Privacy Principles (IPPS) Instruction (Premier and Cabinet circular, 2017)[28]		**Part II Information Privacy Principles** **Use of Personal Information** . . . (8) Personal information should not be used by an agency for a purpose that is not the purpose of collection or a purpose incidental to or connected with that purpose (the secondary purpose) unless: . . . (c) the agency using the information believes on reasonable grounds that the use is ***necessary to prevent or lessen a serious threat to the life, health or safety of the record-subject or of some other person;*** . . . **Disclosure of Personal Information** (10) An agency should not disclose personal information about some other person to a third person for a purpose that is not the purpose of collection (the secondary purpose) unless: . . . (c) the person disclosing the information believes on reasonable grounds that the disclosure is ***necessary to prevent or lessen a serious threat to the life, health or safety of the record-subject or of some other person*** . . .	

Tasmania (Tas)	Personal Information Protection Act 2004	Available to HPs working in the Tas public health setting	**Schedule 1 Personal Information Protection Principles** **2. Use and Disclosure** 1) A personal information custodian must not use or disclose personal information about an individual for a purpose other than the purpose for which it was collected unless — . . . (d) the personal information custodian reasonably believes that the use or disclosure is necessary to lessen or prevent — (i) ***a serious threat to an individual's life, health, safety or welfare . . .*** (Emphasis added.)	Yes *Disclosure of genetic information to at-risk relatives without a patient's consent*. Tasmanian Health Service (2019).[29] Endorse use of NHMRC guidelines to guide exercise of discretion
Victoria (Vic)	Health Records Act 2001	Available to HPs working in the Vic public health setting	**Schedule 1 The Health Privacy Principles** **Principle 2 — Use and Disclosure** . . . 2.2 An organisation must not use or disclose health information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose for which the information was collected unless at least one of the following paragraphs applies — . . . (h) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent — i) ***a serious threat to an individual's life, health, safety or welfare*** . . . and the information is used or disclosed in accordance with guidelines, if any, issued or approved by the Health Complaints Commissioner for the purposes of this paragraph. (Emphasis added.)	No

			Note: Nothing in HPP 2 requires an organisation to disclose health information about an individual. An organisation is always entitled not to disclose health information in the absence of a legal obligation to disclose it.	
Western Australia (WA)	Health Services Act 2016	Available to HPs working in the WA public health setting	**220. Authorised collection, use or disclosure of information** (1) For the purposes of this Act, the collection, use or disclosure of information is authorised if the information is collected, used or disclosed in good faith in any of these circumstances — (i) any other circumstances prescribed for this subsection.	No
	Health Services (Information) Regulations 2017		**5 Circumstances in which collection, use or disclosure of information is authorised (s 220)** (1) For the purposes of section 220(1), the collection, use or disclosure of information is authorised in the following circumstances (a) the collection, use or disclosure is reasonably necessary to lessen or prevent a serious risk to the life, health or safety of any individual . . .	

Footnotes

1. SM Domchek and others "Association of risk-reducing surgery in BRCA1 or BRCA2 mutation carriers with cancer risk and mortality" (2010) 304(9) *Jama* 967; E D Gareth and others "MRI breast screening in high-risk women: cancer detection and survival analysis" (2014) 145(3) *Breast Cancer Research and Treatment* 663.
2. F H Menko and others "Informing family members of individuals with Lynch syndrome: a guideline for clinical geneticists" (2013)12(2) *Familial cancer* 319; S Taylor and others "Family communication following a diagnosis of myotonic dystrophy: To tell or not to tell?" (2019) 28(5) *Journal of genetic counseling* 1029.
3. R B Dugan and others "Duty to warn at-risk relatives for genetic disease: Genetic counselors' clinical experience" (2003) Am J Med Genet C Semin Med Genet; N Meggiolaro and others "Disclosure to genetic relatives without consent — Australian genetic professionals' awareness of the health privacy law" (2020) 21(13) *BMC Medical Ethics*.
4. R McWhirter, C Johnston, J Burke "Disclosure of Genetic Results to At-risk Relatives without Consent: Issues for Health Care Professionals in Australia" (2019) 27(1) *Journal of law and medicine* 108.
5. J Tiller and others "Disclosing genetic information to family members without consent: Five Australian case studies" (2020) 63(11) *Eur J Med Genet*.
6. C Farnos and others *Disclosing genetic information to family members: a comparative law study of the legal regimes applicable to patients' and health professionals' liability* European Society of Human Genetics, Barcelona, Spain 2016.
7. *ABC v St George's Healthcare NHS Trust* [2020] EWHC 455 (QB).
8. E S Dove and others "Familial genetic risks: how can we better navigate patient confidentiality and appropriate risk disclosure to relatives?" (2019) 45(8) *Journal of Medical Ethics* 504.
9. Above n 7.
10. D d'Audiffret Van Haecke and S de Montgolfier "Genetic diseases and information to relatives: practical and ethical

issues for professionals after introduction of a legal framework in France" (2018) 26(6) *European Journal of Human Genetics* 786.

11. B Derbez and others "Familial disclosure by genetic healthcare professionals: a useful but sparingly used legal provision in France" (2019) 45(12) *Journal of Medical Ethics* 811.
12. *Safer v Estate of Pack* 677 A2d 1188; M Weaver "The Double Helix: Applying an Ethic of Care to the Duty to Warn Genetic Relatives of Genetic Information" (2016) 30(3) *Bioethics* 181.
13. M A Rothstein "Reconsidering the duty to warn genetically at-risk relatives" (2018) 20(3) *Genet Med* 285.
14. Table 1, adapted with permission; above nn 4 and 5.
15. S L Keeling "Duty to warn of genetic harm in breach of patient confidentiality" (2004) 12(2) *Journal of law and medicine* 235.
16. MFA Otlowski "Disclosing genetic information to at-risk relatives: new Australian privacy principles, but uniformity still elusive" (2015) 202(6) *The Medical Journal of Australia* 335.
17. Above n 4.
18. See Table 1.
19. National Health and Medical Research Council, *Use and disclosure of genetic information to a patient's genetic relatives under s 95AA of the Privacy Act 1988 (Cth) — Guidelines for health practitioners in the private sector,* Canberra, 2014.
20. See Table 1.
21. See Table 1.
22. Tasmanian Health Service, *Disclosure of genetic information to at-risk relatives without a patient's consent,* Tasmania, 2019.
23. Above n 16.
24. Office of the Victorian Privacy Commissioner *Removal of 'imminent' from the IPPs and HPPs — Guidance for Victorian public sector organisations,* Victoria, 2017.
25. See Table 1.
26. Above n 16.
27. Above n 5.
28. South Australia, *Premier and Cabinet Circular — Information Privacy Principles (IPPS) Instruction* (May 2020) www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf.
29. Above n 19.

The future of data breaches

***Andrea Beatty**, **Chelsea Payne** and **Chloe Kim** PIPER ALDERMAN*

On 11 January 2021, a determination was made by the Australian Information and Privacy Commission compelling the Australian government agency, Department of Home Affairs to pay compensation to victims of a 2014 data breach. This is the first instance where in a representative action a government body has been ordered to compensate victims for non-economic loss arising from a data breach and sets a unique precedent for the future of data breaches and remediation to victims. In light of the review of the Privacy Act 1988 (Cth) (Privacy Act), it poses a question on whether compensation will become a mandatory requirement for non-economic loss resultant from a privacy data breach.

Breach of detainees' privacy

The data breach saw over a thousand asylum seekers' personal information leaked and exposed online through the mistaken uploading of a report *The Immigration Detention and Community Statistics Summary* on the Department of Home Affairs' website. The report revealed personal information such as names, gender, reason for and location of detainment for 9258 individuals who were in immigration detention.[1] As a result of the data breach, a representative complainant on behalf of the asylum seekers brought proceedings against the Department of Home Affairs which Australian Information Commissioner and Privacy Commissioner Angelene Falk was tasked with determining.

Commissioner Falk determined that the Department of Home Affairs should pay compensation for the non-economic loss suffered by class members as a result of the data breach. The quantity of compensation was measured on a scale of five different categories of loss or damage for non-economic loss, depending on the severity of the breaches' impact.[2]

Based on this tiered system, compensation to data breach victims for non-economic loss will range between $500–$20,000 for 1,297 individuals. As mentioned by Commissioner Falk, this was the first instance of victims to non-economic loss being compensated and monetarily reflects the harmful impact the loss of privacy and unwilling disclosure of personal information can have on individuals. The compensation process is expected to occur over a 12-month period during which individual's compensation will be assessed and disbursed to class members.[3]

Is compensation the way of the future?

The significant data breach incident follows on from other recent government data breaches that took place in 2020. One of the most impactful concerned Service NSW, where a breach of 47 employee email accounts saw the government body being forced to apologise to 25,000 people for the disclosure of their personal information through documents including passports and driver's licences.[4] As a result, 3.8 million documents were investigated in 4 months to establish how the breach had occurred and who it affected. However, despite such personal information being revealed as a result of the cyber attack, victims were not compensated for the loss they incurred.[5]

As Commissioner Falk had adopted the five categories of non-economic loss to assess monetary compensations, perhaps such measures will also be adopted for future government breaches as well. This new way of approaching privacy breaches is aligned with the Office of the Australian Information Commissioner's (OAIC's) proposed overhaul of the Privacy Act to ensure the current privacy framework is able to respond to the new challenges posed to privacy in the digital environment. The OAIC's announcement on 30 October 2020 to review the current Privacy Act will be necessary to ensure privacy protections are relevant and adaptable for the future.[6] The emphasis on ensuring protection of personal information is likely to see amendments to how data breaches are treated by the OAIC and following from the recent compensation ordered on the Department of Home Affairs, may incorporate requirements for compensation or a remediation program for victims. Accordingly, the updated legislation may set the tone for more stringent penalties and remediation steps imposed on companies who fail to meet data breach requirements or do not have sufficient mechanisms in place to initially prevent a breach from occurring.

Data breach litigation

Although in the precedent case *ABC v Lenah Game Meats Pty Ltd*[7] the High Court was cautious in recognising a tort of privacy in Australian law, the recent determination made in favour of the class members seems to signify a shift in thinking. Furthermore, whether a statutory tort for serious invasions of privacy should be

implemented into legislation will be a matter to be considered in the OAIC's review of the Privacy Act.[8]

Recently the first proceedings against an AFSL holder for failing to comply with adequate cyber security obligations were commenced by the Australian Securities and Investments Commission (ASIC) against RI Advice Group Pty Ltd (RI Advice Group). ASIC alleged there had been numerous cyber breach incidents at an authorised representative of RI Advice Group and that they did not have the "adequate policies, systems and resources" reasonable to manage the risk in respect of cybersecurity and cyber resilience.[9] Therefore, ASIC sought declarations that RI Advice Group had contravened the Corporations Act 2001 (Cth), ordered RI Advice Group to pay a civil penalty to be determined by court and for RI Advice Group to implement systems that would be reasonably appropriate to adequately manage risk in respect of cybersecurity and cyber resilience.

The imposition of compensation on a government body and legal proceeding brought by a regulatory agency demonstrates the sincerity in which the government and regulatory agencies are treating privacy breaches and the non-economic loss to individuals consequent from it. Accordingly, it seems there may be a shift in the way privacy breaches are currently dealt with to one which puts the onus on government bodies and companies to comply with data breach requirements or face orders requiring monetary compensation.

Andrea Beatty
Partner
Piper Alderman
abeatty@piperalderman.com.au
www.piperalderman.com.au
www.andreabeatty.com.au

Chelsea Payne
Associate
Piper Alderman
cpayne@piperalderman.com.au
www.piperalderman.com.au

Chloe Kim
Lawyer
Piper Alderman
ckim@piperalderman.com.au
www.piperalderman.com.au

Footnotes

1. C Knaus "Australian government ordered to pay 1,300 asylum seekers whose details were exposed" *The Guardian* 27 January 2021, www.theguardian.com/australia-news/2021/jan/27/australian-government-ordered-to-pay-1300-asylum-seekers-whose-details-were-exposed.
2. *"WP" and Secretary to the Department of Home Affairs (Privacy)* [2021] AICmr2 (11 January 2021).
3. Above.
4. Service NSW, Service NSW cyber incident, www.service.nsw.gov.au/cyber-incident.
5. Lucy Cormack "Service NSW data breach affected 80,000 fewer people than first thought" *Sydney Morning Herald* 16 December 2020, www.smh.com.au/national/nsw/service-nsw-data-breach-affected-80-000-fewer-people-than-first-thought-20201215-p56np7.html.
6. OAIC, "OAIC welcomes Privacy Act review", media release (30 October 2020) www.oaic.gov.au/updates/news-and-media/oaic-welcomes-privacy-act-review/.
7. *Australian Broadcasting Corp v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199; 185 ALR 1; [2001] HCA 63; BC200107043.
8. Attorney-General's Department, *Terms of Reference*, www.ag.gov.au/system/files/2020-10/privacy-act-review-terms-of-reference.pdf.
9. Federal Court of Australia, *Australian Securities and Investments Commission v RI Advice Group Pty Ltd (ACN 001 774 125)* Statement of Claim (2020), https://download.asic.gov.au/media/5836071/20-191mr-2020-10-26-vid-556-asic-v-ri-soc-filed.pdf.

Privacy and inclusivity by design: how to protect the privacy of children and vulnerable people

Alec Christie *and* ***James Wong*** *CLYDE & CO*

Introduction

There is widespread recognition that privacy protections for children and vulnerable people must be strong and likely stronger (or the same measures applied differently) than for others. Privacy is a key thread that runs through the *United Nations Convention on the Rights of the Child*, which for children requires the protection of identity, access to information, communications, reputation (or "good name") and seeks to safeguard against physical risks (eg sexual abuse, harmful work, trafficking and exploitation) and discrimination. The same is true of similar international instruments relating to other Vulnerable Persons (defined below) in which privacy plays a supportive role in the expression of other human rights and interests.

However, the Privacy Act 1988 (Cth) including the Australian Privacy Principles (collectively, APPs) is broadly agnostic as to individuals who are young, old, infirm, have a limited grasp of English or have other characteristics that may render them vulnerable (Vulnerable Persons).

The current position in Australia

The Office of the Australian Information Commissioner (OAIC) has provided some limited guidance[1] but, in the absence of univocal "rules" or requirements under the APPs, it is difficult to determine how to implement the requirements of the APPs in relation to all Vulnerable Persons in practice, at least to the same level of protections/rights offered generally under the APPs. As well as implementing the APPs requirements in practice for Vulnerable Persons, organisations should consider what standard the community expects and/or what steps must be taken to be a good privacy "citizen" as regards Vulnerable Persons.

eSafety considerations

In parallel to any applicable privacy protections, the Enhancing Online Safety Act 2015 (Cth) established the office of the eSafety Commissioner, who has various statutory functions and powers that foster online safety and, in practice, operate to protect children and some other Vulnerable Persons. These functions and powers are directed against cyberbullying, the non-consensual sharing of intimate images and the removal of abhorrent violent material (AVM). Online services that could be used for cyberbullying, sexting or the sharing of child sexual abuse material or AVM should, at a minimum, be aware of the eSafety Commissioner's powers of investigation, enforcement and handing down of *ad hoc* directions. Owners and operators of digital platforms must stay abreast of developing risks relating to eSafety and proactively take steps to protect children and other Vulnerable Persons from harm.

Going beyond "personal information"

In the Final Report for the *Digital Platforms Inquiry*, the Australian Competition and Consumer Commission (ACCC) recommended expanding the definition of "personal information" under the APPs in line with changing consumer expectations and, more broadly, to reform Australian privacy law to correct the power imbalance and information asymmetry between digital platforms and consumers.[2] This is currently being considered as part of the present review of the Privacy Act.[3] As a result, we may see greater protections for inferred, anonymised and de-identified information, which are becoming increasingly powerful tools for business decision-making, sometimes to the detriment of Vulnerable Persons because they can be used to generate (often unfair or discriminatory) assumptions or predictions about a person on the basis of certain attributes. Any regulatory reform in this direction will align with the global trend of extending privacy obligations to more categories of information. In the meantime APP entities should be preparing for more onerous privacy protections, particularly as applicable to Vulnerable Persons.

Requirements under the APPs

As is well known, the APPs set out principles to protect an individual's personal information and provide them certain rights in respect of such, regardless of their

age or markers of disadvantage or vulnerability. That is, the APPs apply to all and equally to all, regardless of race, class or creed (a fundamental tenet of the "rule of law"). However, this ignores the reality that certain groups in our society are less able to exercise their rights and more likely to suffer harm (or will suffer greater consequences from a harm) by reason of, for example, their ethno-cultural background, refugee status, membership of a persecuted group, mental or physical incapacity, ill-health and/or lived experience of violence or abuse (in this article, all Vulnerable Persons). Currently, the privacy protections afforded by the APPs do not specifically account for such differences.

Consent (as defined below) is the central principle on which the APPs are based. An individual must have the "capacity" to consent if that consent is to be valid under the APPs. Capacity is therefore a key element on which the extent of privacy protections provided to Vulnerable Persons turn. To have *capacity* means the individual:[4]

- understands that they are being asked to decide whether to give or withhold their consent
- understands the consequences of giving or not giving their consent
- bases their decision on reasoned judgement, and
- can communicate their consent decision

An individual may not have capacity to consent where they are aged under 18 years, have a physical or mental disability, are temporarily incapacitated or have a limited understanding of English.[5] The OAIC notes that, under the APPs, APP entities must determine on a case-by-case basis whether an individual under the age of 18 years has the capacity to give consent.[6] However, while other categories of Vulnerable Persons are not specifically addressed, surely the same principle applies. That is, for any Vulnerable Person, APP entities must determine their capacity to consent.

Why Vulnerable Persons need different (or differently applied) privacy protections

Whether in relation to criminal culpability, family law, advertising content, contracting or employment protections, a multitude of laws and regulations in Australia adapt protections or the means of exercising them for Vulnerable Persons.

The APPs are centred on the capacity to be notified of (ie access and understand) a privacy notice, consent to certain activities in some specific cases (eg sensitive information) and to exercise choice (whether or not to provide one's personal information on such terms) and/or one's rights under the APPs (collectively, consent). In many instances, just like in other areas of law, Vulnerable Persons will not be in the same position as others to make a "good" choice, provide "good" consent or fully exercise their rights (ie, exercise consent as we have defined it) under the APPs. Furthermore, a data breach involving personal information may have a greater impact on a Vulnerable Person (and may cause serious harm where it may not if the affected individual was not a Vulnerable Person).

However, compared to explicit protections for Vulnerable Persons entrenched in other areas of law (including means to make complaints or seek redress), in the case of privacy rights under the APPs, there is something of a gap in the level of practical protections afforded to Vulnerable Persons. In the absence of specific protections in the APPs, better practice dictates a greater onus on the APP entity processing personal information to consider (and seek to better protect) Vulnerable Persons' privacy and rights under the APPs.

New technologies and emerging norms for the use of personal information also significantly elevate privacy risks for Vulnerable Persons. For example, as profiling and automated decision-making move into the mainstream, applied to everything from the targeting of consumer goods to accessing government services, there is an increasingly tangible cost to the autonomy of individuals who are part of any group that is targeted (or discriminated against). As machine learning becomes a staple of such profiling and/or automated decision-making, adverse targeting (and discrimination) could be entirely inadvertent or simply reflective of real-world discrimination/biases. In any case, Vulnerable Persons may not be in a position to fight back against such bias or fully assert the rights given to individuals generally under the APPs.

Future directions internationally

As the digital economy rapidly advances and the risks of harm to Vulnerable Persons grow, we expect to see more specific privacy obligations imposed in the near future both in Australia and globally. Policy approaches around the world reflect this trend and provide an indication of possible future directions.

The United States is the only national jurisdiction that has enacted bespoke legislation for the protection of children's privacy in the form of the Children's Online Privacy Protection Act of 1998 (US) (COPPA). COPPA regulates operators of websites and online services directed at children under the age of 13 years or that collect personal information from children under the age of 13 years. COPPA includes obligations to publish a privacy notice, provide certain information to parents, obtain verifiable parental consent before collecting a child's personal information and give parents certain choices as to the holding, use and disclosure of their child's personal information.

The Office of the Privacy Commissioner of Canada (OPC) has taken early steps to protect Vulnerable Persons' privacy through the identification of inappropriate purposes for collection, use and disclosure of personal information (so called "no-go zones"), including:

- collection, use or disclosure that is otherwise unlawful (eg, using credit score information for the delivery or targeted ads)
- profiling or categorisation that leads to unfair, unethical or discriminatory treatment contrary to human rights law (eg, using big data to draw inferences about individuals or groups) and
- collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual

In the United Kingdom, 2020 saw the introduction of the *Age Appropriate Design Code* (AADC) under the Data Protection Act 2018 (UK).[7] The AADC applies to organisations providing online services likely to be accessed by children in the United Kingdom and requires that such services take into account the best interests of the child. It sets out 15 standards of age-appropriate design reflecting a risk-based approach, striving towards data minimisation through the use of privacy-respecting default settings. Under the AADC, children may be allowed to change their default settings but only if they are given the right information, guidance and advice before they do so and are afforded proper protections as to how their data is used thereafter. Design requirements are based on a child's developmental stages; you need to tailor your online service to each age group that may use it.

It remains to be seen which, if any, of these approaches might be incorporated into Australian privacy law. However, the current review of the Privacy Act[8] puts into sharp focus the issues of how privacy information is presented to Vulnerable Persons and their capacity to accept notice and provide consent. Until these developments find their way into specific provisions of the APPs the question remains one of how best to meet the overarching obligation under the APPs to ensure capacity to consent.

What can you do now?

Considering incapacity to consent

According to the APP Guidelines, if an APP entity is "uncertain as to whether an individual has capacity to consent at a particular time, it should not rely on any statement of consent given by the individual at that time".[9] That is, in certain circumstances (ie, for Vulnerable Persons), the individual should be treated as unable (ie, lacking capacity) to consent in the usual manner and any consent provided by the individual cannot be relied on as a basis for collecting, using or disclosing their personal information. Instead, the APP entity should consider whether and how notice can best be given and consent obtained. This might be with or through the support of an interpreter, alternative communication methods and/or someone acting on the individual's behalf (eg, a parent or guardian)[10] or other means as suggested by Vulnerable Persons themselves. However, even in circumstances where someone else is acting on behalf of the Vulnerable Person, the Vulnerable Person must be involved as far as practicable in any decision-making process about their personal information.[11]

The clearest guidance for obtaining valid consent from children is found in the APP Guidelines which state that an individual aged 18 years or over has the capacity to consent "unless there is something to alert it otherwise".[12] However, for individuals under the age of 18 years (ie, children), the APP entity must determine on a case-by-case basis whether the child has "sufficient understanding and maturity to understand what is being proposed".[13] Of course, in the online world, it is rarely practicable to perform case-by-case assessments of children's capacity to consent. So, as a rule of thumb, for children aged under 15 years, you *must* presume they do not have the capacity to consent and require consent from a parent or guardian.[14] For children aged 15 to 17 years, you may, as a rule of thumb, presume they have the capacity to consent "unless there is something to suggest otherwise".[15]

An example of putting this into practice is that a privacy policy for an online platform used by children (but not targeted towards at-risk children) might prominently include the following notice:

> *If you are aged 14 years or under you must refer this Privacy Policy to a parent/guardian and obtain their consent to us collecting, using and disclosing your personal information in accordance with this Privacy Policy. You* ***must*** *do this before you access the [Platform].*

A privacy policy for an online platform used by Vulnerable Persons other than children, for example, might include the following accessible notice:

> *Please ask us for help [and state how — by several alternative means] if you:*
> - *find it hard to access, read or understand this Privacy Policy; or*
> - *you don't know what it means for you.*

Equal opportunity

Armed with large volumes of personal information, digital platforms are increasingly able to target advertisements and make decisions (eg, eligibility for a financial product) based on certain characteristics of a

person. This can fall foul of equal opportunity legislation, restrict the autonomy and adversely impact the interests of already vulnerable persons such as the elderly, ethnic minorities and those suffering from a mental or physical disability. Discrimination, including through the use of personal information for profiling, entrenches social disadvantage.

In this vein, while privacy laws around the world (including the APPs), focus on the identifiability of an individual, privacy harms can also arise from "individuation" ("the ability to distinguish one individual from others, even if that individual's identity is not known"):[16]

> From the digital breadcrumbs we leave behind in the form of geolocation data shed from our mobile devices, to the patterns of behaviour we exhibit online as we browse, click, comment, shop, share and 'like', we can be tracked. Tracked; then profiled; and finally targeted . . . all without the party doing the tracking, profiling or targeting needing to know 'who' we are.[17]

Individuation can be hidden behind terms such as "tailoring" and "personalising" services or experiences. However, as Johnston rightly concludes:[18]

- decisions are made about who sees what, and equally what will be withheld from whom and this facilitates discrimination, and
- micro-targeted advertising gives rise to the risk of organisations preying on vulnerable individuals

While the APPs do not currently explicitly proscribe such conduct, Australian equal opportunity and anti-discrimination laws will apply in many (but not all) scenarios.

At the federal level, the Age Discrimination Act 2004 (Cth), Racial Discrimination Act 1975 (Cth) and Disability Discrimination Act 1992 (Cth) prohibit discrimination on the basis of age, race and disability status respectively in, most relevantly to digital platforms, the provision of services. All eight state and territory jurisdictions have equal opportunity and anti-discrimination laws that prohibit discrimination on the basis of certain protected personal characteristics. Organisations that provide services in Australia, including online services, must ensure that any uses and disclosures of personal information for or in support of profiling and/or automated decision-making comply with all equal opportunity and anti-discrimination laws.

"Inclusive design" meets privacy by design

Better practice in 2021 is to include "inclusive design" in your privacy by design program, incorporating into the design of a service the fullest possible range of human diversity, including with respect to age, ability, culture and English language proficiency. This reflects an evolution from an early focus on "accessibility" and accommodating for users with disabilities.[19] As an emerging discipline, practitioners have not yet agreed on a definition of inclusive design. However, the University of Cambridge explains it as follows:

> Inclusive design emphasizes the contribution that understanding user diversity makes to informing these decisions, and thus to including as many people as possible. User diversity covers variation in capabilities, needs and aspirations.[20]

The Centre of Inclusive Design (formerly Media Access Australia) proposes three dimensions of inclusive design as follows:[21]

(1) recognise diversity and uniqueness, because "most individuals stray from the average in some facet of their needs or goals"
(2) inclusive process and tools — which includes involving individuals who have a lived experience as the "extreme users" a service may be used by, and
(3) broader beneficial impact — an acknowledgment that the benefits of a service flow beyond the "end" users of the service given those end users may use the service to serve users further downstream

Privacy practitioners are aware that privacy by design mandates the incorporation of privacy principles into the design of a products and services (ie, privacy cannot be a "bolt-on" at the end). In 2021, privacy considerations including principles of inclusive design should be embedded into almost every aspect of user experience (UX) design — even choosing the size and boldness of fonts and use of colour. For instance, the ACCC recently launched an action against Google for allegedly misleading consumers and nudging them (especially the more vulnerable) to give away substantially more personal information than they believed they were actually choosing (ie, consenting) to — this being achieved partly through "clever" presentation of information next to an "I agree" button.[22]

We think the above sentiments reflect the trajectory of community expectations too. Consumers are increasingly willing to both: (i) "call out" and penalise service providers that (often without malice) fail to incorporate inclusive design principles; and (ii) applaud and reward service providers that appear to champion these principles.

Inclusive design, in the context of privacy, means providing for Vulnerable Persons as much as is practicable in the design of privacy for the products and services and their delivery. Common manifestations include the integration of assistive technology (eg, screen reading functionality, magnified text and high-contrast options for the presentation of privacy notices and prompts for the giving of consent). However, the key is

to go through a structured process of thinking carefully about the particular privacy needs of likely users of a service or product and, dare we say it, asking users who are Vulnerable Persons how they would prefer to have their privacy protections and rights met.

Conclusion

Remember, while often forgotten, the APPs do impose an overarching obligation on APP entities to determine whether the relevant individual has the capacity to consent. Of course, case-by-case assessment is usually impracticable so assumptions about the capacity of users are often applied. However, APP entities need to be aware of any indications that the individual does not have capacity to consent, especially where there is an expectation of processing the personal information of Vulnerable Persons.

In an emerging landscape where trust is paramount and privacy is as much about ethics as compliance, until specific requirements are added to the APPs, organisations should consider how they can exemplify fairness, accountability and transparency in the collection, use and disclosure of the personal information of Vulnerable Persons. Maybe it is a case of different processes, policies and "rules" for Vulnerable Persons (or different application of them) in order to address any material detriments resulting from the application of uniform processes, policies and "rules" to all. Also, remember, what is voluntary "better practice" today is likely to become mandatory in the imminent future.

Alec Christie
Partner
Clyde & Co
Alec.Christie@clydeco.com
www.clydeco.com

James Wong
Associate
Clyde & Co
James.Wong@clydeco.com
www.clydeco.com

Footnotes

1. OAIC, *Australian Privacy Principles Guidelines — Privacy Act 1988* (July 2019), www.oaic.gov.au/assets/privacy/app-guidelines/app-guidelines-july-2019.pdf.
2. ACCC *Digital platforms inquiry — final report* (June 2019) www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf.
3. Attorney General's Department, Review of the Privacy Act 1988, www.ag.gov.au/integrity/consultations/review-privacy-act-1988.
4. OAIC, Consent to the handling of personal information, www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/consent-to-the-handling-of-personal-information/#CapacityToConsent; Above n 1, at B.52.
5. OAIC, above; Above n 1, at B.53.
6. Above n 1, at B.56.
7. Information Commissioner's Office, Age appropriate design: a code of practice for online services, https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/.
8. On 12 December 2019, the Commonwealth Attorney-General announced a review of the Privacy Act as part of the Australian Government's response to the ACCC's Digital Platforms Inquiry. See above n 3.
9. Above n 1, at B.52.
10. Above n 1, at B.54.
11. Above n 1, at B.55.
12. Above n 1, at B.52.
13. Above n 1, at B.57.
14. Above n 1, at B.58.
15. Above.
16. A Johnston "Reforming privacy laws to protect against digital harms" (2021) 93 *Computers & Law* 38, at 38.
17. Above.
18. Above n 16, at 40.
19. See for example the World Wide Web Consortium, Web Content Accessibility Guidelines (WCAG), www.w3.org/WAI/standards-guidelines/wcag/.
20. University of Cambridge, Inclusive Design Toolkit, www.inclusivedesigntoolkit.com/whatis/whatis.html.
21. Centre for Inclusive Design, Inclusive Design, https://centreforinclusivedesign.org.au/index.php/resources/inclusive-design/.
22. ACCC "Correction: ACCC alleges Google misled consumers about expanded use of personal data" media release (27 July 2020) www.accc.gov.au/media-release/correction-accc-alleges-google-misled-consumers-about-expanded-use-of-personal-data.

For editorial enquiries and unsolicited article proposals please contact Genevieve Corish at genevieve.corish@lexisnexis.com.au or (02) 9422 2047
Cite this issue as (2021) 17(9) *PRIVLB*
SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au
SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067
CUSTOMER RELATIONS: 1800 772 772
GENERAL ENQUIRIES: (02) 9422 2222
ISSN 1449-8227 Print Post Approved PP 243459/00067