31 March 2023

Australian Government Attorney-General's Department
By email: PrivacyActReview@ag.gov.au

Review of the Privacy Act

About us

The **UNSW Allens Hub for Technology, Law and Innovation** ('UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

About this Submission

We are grateful for the opportunity to make a submission on the Privacy Act Review Report 2022. Our submission reflects our views as researchers; they are not an institutional position. This submission can be made public.

We do not address the proposed reforms as a whole, but rather focus on areas on which our research can shed light. Our main points relate to:

- Careful consideration for introducing a criminal offence for malicious re-identification of de-identified personal information;
- Encouraging standardisation that would make privacy policies 'machine-readable';
- Ensuring that privacy-by-default guidance captures web cookies;
- Stronger OAIC intervention powers in relation to identified high privacy risks;
- Taking a more technology-neutral approach to the problems said to be associated with automated decision-making;
- Reconsidering the consequences associated with a child's consent and retaining the exception to prohibiting targeting children;
- The benefits of one civil penalty provision for all interferences with privacy over the proposed tiers of civil penalty provisions;
- Reconsidering the introduction and application of infringement notices to the *Privacy Act*;
- The need for up-to-date OAIC guidance on identification and mitigation of reasonably foreseeable risks or losses to individuals from an interference with privacy, so that as additional steps develop they are adopted as part of best practice;
- APP entities should receive credit in the form of reduced penalties for pro-active steps for identifying and mitigating foreseeable risks';

- The need for legislation to provide examples of particular orders that may be made by courts after a civil penalty provision relating to an interference with privacy has been established;
- The importance of sufficient funding for the Australian public to have an effective privacy regulator;
- Further consideration of the circuitous route contained in the design elements for a Direct Right of Action;
- Addressing the co-existence of multiple routes to compensation under a direct right of action, within the *Privacy Act* and other legislation;
- Adding a statutory compensation model for minor losses and to encourage compliance;
- Expanding the Notifiable Data Breaches (NDB) scheme;
- Harmonising cyber security regulation, including privacy law.

We also encourage the government to explore how 'data problems' might be resolved outside of privacy and data protection laws.[1] While that is beyond the scope of this Review, government can begin thinking more long term about how law can protect people from data-related harms in ways that go beyond regulation of data processing. Ideas include reforms to discrimination law so that it protects against biases associated with data-driven decision-making and expanding the role of human rights protections.

Proposal 4 De-identified Information

Proposal 4.5 accurately acknowledges that de-identification is a process and that the ability to identify an individual from data that has gone through that process is context-specific.

Proposal 4.6 would ensure that APP entities retain some responsibility for the protection of de-identified information. These are framed so as to only require 'reasonable' steps – allowing for a risk-based approach that depends on the contextual likelihood of re-identification.

We agree that both proposals are an improvement on the current situation where information can be 'de-identified' and then placed outside the remit of the legislation. However, we note that the proposal adds complexity compared to an expanded definition of 'personal information' as proposed by Salinger Privacy. In particular, it adds a new box, rather than recognising that there is a multi-dimensional spectrum with different levels of identifiability and individuation.

We are particularly concerned about the potential scope of prohibitions on re-identification. The example of someone re-identifying de-identified information to demonstrate the failure of organisations to comply with obligations proposed in **Proposal 4.6** highlights the importance of carefully crafting any criminal offence for 'malicious re-identification' under **Proposal 4.7**. If an offence is introduced, the 'seek to cause harm' test should be limited to harm to the re-identified data subjects, not to the APP entity (that may justifiably suffer reputational harm because of publicity of the lack of sufficient protections). An exception for security researchers should thus also cover internal whistle-blowers, who may be perceived as 'malicious' from the perspective of the APP entity.

[1] Lyria Bennett Moses and Kimberlee Weatherall, 'Data problems and legal solutions – some thoughts beyond privacy', *Data and the Digital Self* (ACS 2023).

Proposal 10.3 Standardised Templates

While we agree with proposal 10.3 for increased standardisation in privacy policies and collection notices, we encourage guidance/APP Codes to also consider standardisation that would facilitate machine-readable privacy policies. This goes beyond standard word formulas and icons to explore (either generally or in particular industries) ways to make privacy settings 'searchable'. This would be particularly useful to consumers in online settings, where it is already possible, for example, to search for images based on standard licensing conditions or to search apps based on the data they collect. At the very least, we encourage those developing relevant guidelines and codes to consider this possibility.

Proposal 11.4 Privacy by Default

We support this proposal. Given that the GDPR has not led to privacy-by-default in practice in the context of website cookies and associated techniques, the OAIC's proposed guidance should include examples in that context.

Proposal 13 Additional Protections

The recommendation that Privacy Impact Assessments (PIAs) be provided in cases with high privacy risks is welcome, as it goes some way to overcoming problems with 'corporate opacity' in relation to the collection, analysis, use and dissemination of data.[2] However, we would support stronger intervention powers by the OAIC rather than mere 'guidance' in relation to identified high privacy risks. Guidance by the OAIC has not previously been very effective in changing the conduct of businesses, most notably in failing to encourage appropriately voluntary, informed, current and specific consent.[3] The weakness of guidance compared to stronger regulation, particularly in the case of technology, is not confined to privacy protections in Australia, but can be seen as a wider problem.

The 'product intervention powers' proposed by the Consumer Policy Research Centre in their recent report[4] provide a stronger model for dissuading corporate misconduct (particularly of large digital platforms) in relation to their handling of personal information.

Proposal 19 Automated Decision Making (ADM)

The problem with Proposal 19 is that it introduces a technology-specific law to solve a problem that is not necessarily linked to that technology. There are a variety of issues that people are concerned

[2] Zofia Bednarz and Kayleen Manwaring, 'Hidden depths: The effects of extrinsic data collection on consumer insurance contracts' (2022) 45 *Computer Law & Security Review* Art 105667, 4-5.

[3] Kayleen Manwaring, '"Click Here to (Dis)agree": Australian Law and Practice in Relation to Informed Consent' (2022) 3(3) *Global Privacy Law Review* 127, 129ff.

[4] Chandni Gupta (Consumer Policy Research Centre), 'In whose interest? Why businesses need to keep consumers safe and treat their data with care' (*CPRC Working Paper*, March 2023).

about around ADM and Artificial Intelligence (AI), but that does not imply that the best way to deal with these is through technology-specific law.[5]

The initial discussion of ADM in the Report recognises the distinction between ADM and AI, which can operate with varying levels of automation (including none at all). However, in discussing the risks, the Report does not clearly distinguish between risks associated with automation and risks associated with machine learning and data-driven inferencing. They are quite distinct.

The risks associated with automation were evident in Robodebt: flawed decision-making at scale. The risks associated with machine learning and other forms of data-driven inferencing are distinct and can arise even where a decision-making process is not automated. For example, the reliance on risk assessment tools in the criminal justice system is often very manual, including human psychologists giving evidence about their use of particular tools and human judges factoring that evidence into sentencing decision. Nevertheless, the problems discussed in the Report (including training systems on historic data affected by prejudice) apply in this example *despite the lack of relevant automation*.[6] Indeed, if the same data-driven decision-making was done without computers at all (relying instead on statistical modelling by humans), *exactly the same problems would arise* with respect to bias. 'Algorithmic bias' blames the machine, but the problem is in how data is collected, how inferences are made and then applied inappropriately. AI makes the use of data-driven inferencing more common, but they are not the same thing and neither necessarily involves ADM.

In light of this distinction, it is worth considering what Proposal 19 is addressing. If the focus is on ADM and automation, then it cannot fix 'algorithmic bias' except in an artificially narrow set of circumstances. Whether notification is required will be *technology-specific*, depending on the mechanism through which decisions are made rather than the type of reasoning involved in the decision. One could deal with 'algorithmic bias' elsewhere (say, in rules restricting profiling) but this is like whack-a-mole. The regulatory target needs to align with the regulatory goal. ADM is the thing many people are worried about, but when you look more deeply into what the problem is, much is independent of the extent to which processes are automated. If data-driven decision-making, and resulting bias, is the problem, you cannot fix it by rules about automation.

An alternative would be to adopt a technology-neutral approach. This would require privacy policies to set out the types of personal information that would be used in *any* decisions that have a legal, or similarly significant effect on an individual's rights. That would ensure that data subjects are aware that disclosing data may lead to decisions that affect their legal or similar rights, independent of the technological tools used in making that decision. It would provide a warning about data-driven inferencing, and hence profiling and bias, or automation, wherever these may occur.

In addition, if there are concerns specifically related to ADM, they could be dealt with in a technology-specific way (i.e., a rule that only applied to ADM). This would, however, relate more

[5] See generally Michael Guihot and Lyria Bennett Moses, *Artificial Intelligence, Robots, and the Law* ch 10 (LexisNexis 2020).

[6] Julia Angwin and others, 'Machine Bias' [2016] ProPublica <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 6 August 2018; Michael Guihot and Lyria Bennett Moses, *Artificial Intelligence, Robots, and the Law* (LexisNexis 2020).

specifically to concerns about scale, or lack of human involvement in or on the loop. Regulation of ADM is not a suitable means to manage concerns about bias.

Proposal 20 Direct Marketing, Targeting and Trading

Proposal 20.5

Introducing specific restrictions on direct marketing to children is a welcome step. The report states that direct marketing is unlikely to cause harm when the personal information is collected directly from the child, such as them signing up for a mailing list for an activewear brand, but receiving information about the brand's new range of diet supplements would not be in the child's best interests.[7] However, mailing lists are not limited to goods for sale and may include influential informational products such as Substack newsletters.[8] Further consideration is thus required to determine what consequences should be attached to a child's consent, which relates to the burden that can be placed on children to regulate what is in their best interest. In some circumstances, it may be appropriate to use different consent forms for children and adults, and attach different consequences to each.

Proposal 20.6

The proposal to prohibit targeting to a child, with an exception for targeting that is in the child's best interests, is conducive for providing a safe online environment for those aged under 18. We recommend reconsidering the exception once the 'child's best interests' have been defined, because the exception may in fact not be of benefit. For instance, the report cites the example of 'services that may be beneficial for children and pose little privacy risk, such as music streaming services that provide personalised music recommendations based on the profiling of a child's past listening activity and predicted music interests.'[9] However, such profiling may be harmful to children by reducing the extent to which they learn and explore through serendipitous encounters. Moreover, if such targeting is to be permitted, it should be an opt-in choice and not the default setting.

Proposal 20.8

This proposal would be a positive step towards safeguarding individuals' online privacy. In light of the CDEI Online Targeting Report's finding that of '...a desire for individuals to be able to exercise more control over the way they are targeted',[10] we support an opt-in choice. This reduces the burden on users to opt-out and provides for privacy-by-default.

Proposal 20.9

This proposal requires entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals. There will need to be clear guidance on what information is required, so that entities are not left to make their own

---

[7] Attorney-General's Department, *Privacy Act Review* (Report, 2022) 215.

[8] Falon Fatemi, 'The Rise of Substack – And What's Behind It', *Forbes Business* (Article, 20 January2021) <https://www.forbes.com/sites/falonfatemi/2021/01/20/the-rise-of-substack-and-whats-behind-it/?sh=f5825ca159f4>.

[9] Attorney-General's Department, *Privacy Act Review* (Report, 2022) 216.

[10] Centre for Data Ethics and Innovation (UK), *Online Targeting: Final Report and Recommendations* (04 February 2020) 04.

decisions about what to leave out. Even the term 'algorithms' is ambiguous here, as it is not clear whether it is limited to the use of computers or includes the following of any process that yields an output. But, more broadly, privacy policies are often hard to find and difficult to interpret – if there is to be change here, it will need to come from clear requirements in law.

Additionally, where targeting is not the primary purpose of a product or service, individuals should be able to choose whether they want to opt-in or not for their personal information being used, collected, and disclosed for targeting. This should eliminate the scope of data-grab, which involves asking consumers more information about themselves than what is required to access a product/service, as reported by the Consumer Policy Research Centre.[11]

Lastly, the premise of **Proposal 20** appears to be that individuals' personal information needs to be compromised for entities' economic benefit. Studies have shown that targeted advertising can affect human behaviour; Summers, Smith, and Reczek[12] found that behaviourally targeted advertisements can change individuals' self-perceptions, and these changes can extend beyond their purchase intentions. We suggest considering alternatives to mitigate such impact. For instance, making it mandatory for consumers to have the option to pay a fee for a product or service instead of it being free of cost and relying on data collection, use, and disclosure for their revenue.

Proposal 25 Enforcement

Effective enforcement needs the following elements:

- Sufficient funding;
- A regulator with expertise;
- Investigatory powers to be able to obtain information and assist in proving contraventions;
- An enforcement pyramid with sufficient steps or enforcement tools to allow the regulator to adopt an appropriate response; and
- For the higher levels in the enforcement pyramid, penalties that are sufficiently large that it is worthwhile for a regulator to incur the higher costs in seeking a penalty.[13]

It should also be remembered that enforcement is not just public enforcement by a government regulator; we live in an age of regulatory pluralism. Regulated entities may be encouraged to alter their behaviour because of a range of influences. Of particular importance is private enforcement in the form of civil litigation, including through the representative proceeding or class action.

Proposal 25.1

This submission endorses the proposed reform's aim of increasing the range of enforcement mechanisms. However, the proposal of tiers of civil penalty provisions is unnecessary, over-complicates the legislation and restricts the OAIC's discretion as to the appropriate penalty to seek. We agree with the OAIC view that there should be one civil penalty provision for all interferences

[11] Consumer Policy Research Center, *Duped by Design* (Final Report, June 2022) 25.

[12] Christopher A Summers, Robert W Smith and Rebecca Walker Reczek, 'An Audience of One: Behaviourally Targeted Ads as Implied Social Labels' (2016) 43(1) *The Journal of Consumer Research* 156, 171.

[13] Michael Legg, *Public and Private Enforcement of Securities Laws* (Hart, 2022) 216.

with privacy and that it would then be for the Court to consider the nature and extent of the contravention in determining the penalty.

ASIC and the ACCC have the ability to bring civil penalty proceedings in a range of circumstances. There are no tiers, just a maximum amount for each contravention. The amount imposed for a civil penalty is subject to statutory criteria and a well-developed case law (from a range of regulatory regimes) but which requires court determination, or approval in the case of a settlement. The amount of the penalty needs to be in a range that is commensurate with the misconduct. In the civil penalty context, the Full Court of the Federal Court explained the process as follows:

The fixing of a pecuniary penalty involves the identification and balancing of all the factors relevant to the contravention and the circumstances of the defendant, and making a value judgment as to what is the appropriate penalty in light of the protective and deterrent purpose of a pecuniary penalty.[14]

The *Regulatory Powers (Standard Provisions) Act 2014 (Cth*) s82(6) similarly states that "the court must take into account all relevant matters".[15]

It is unclear why privacy needs to be dealt with in a different manner from consumer, competition or securities contraventions.

Infringement notices have a role in the enforcement pyramid, but reference should be made to the final report of the *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry* which critiqued their use.[16] As Commissioner Hayne observed, infringement notices were originally designed for use with minor criminal offences. However, more recently their use has expanded, including in relation to civil penalty provisions.[17] While the infringement notice can address non-compliance in a speedy manner they are "unlikely to have any real deterrent (or punitive effect)".[18] Indeed they can undermine effective enforcement if over-used by a regulator, especially when a more serious response is needed. As Commissioner Hayne stated, the infringement notice can encourage regulated entities to see non-compliance with the law as a cost of doing business.[19] If infringement notices are to be added to the *Privacy Act*'s enforcement pyramid they should apply only to clear administrative contraventions.

---

[14] *Australian Building and Construction Commissioner v Construction, Forestry, Mining and Energy Union* [2017] FCAFC 113; 254 FCR 68, [100]. See also *Flight Centre Ltd v Australian Competition and Consumer Commission* (No 2) [2018] FCAFC 53; 260 FCR 68, [55] ('the task is one that is evaluative, taking into account all the circumstances of the case, not to be reached mechanically or by some illusory process of exactitude, but rather by evaluation that is articulated to a point (but no further) that is useful and meaningful.'); *Australian Securities and Investments Commission v Westpac Banking Corporation* [2019] FCA 2147, [261].

[15] See *Commissioner of Taxation v Balasubramaniyan* [2022] FCA 374.

[16] *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry* (Final Report – Volume 1, 2019).

[17] Ibid 436-439.

[18] Ibid 438.

[19] Ibid 439.

Proposal 25.3

Effective enforcement requires that a regulator have sufficient investigatory powers to be able to obtain information and assist in proving contraventions. The application of Part 3 to the *Regulatory Powers (Standard Provisions) Act 2014* (Cth) to investigation of civil penalty powers is appropriate.

Proposal 25.5

Identification and mitigation of reasonably foreseeable risks or losses to individuals from an interference with privacy is an important step in reducing the impact on a person's privacy. It is a more proactive response than simply waiting to see whether loss occurs and then attempting to redress it. Prevention is preferable, especially when more serious losses may not eventuate until after a significant amount of time has passed, or result from the combination of multiple sources of private information.

The Report provides the following examples of identification and mitigation:

> such as monitoring whether information of the subject of an eligible data breach has been published for sale on the dark web, paying for a credit monitoring service that alerts affected individuals if there are changes to their credit report, assisting individuals to replace compromised credentials such as drivers licences and passports, and engaging service providers such as identity theft and cyber support providers to provide post-incident support to individuals.

We agree that OAIC guidance on the steps that could be taken would be useful. Importantly, that guidance needs to remain up-to-date so that as additional steps develop they are adopted as part of best practice.

We also recommend that an APP entity that undertakes these pro-active steps receive credit for them in relation to amount of a civil penalty or compensation that is ordered to be paid.

The inclusion of mitigating steps in a determination may also impact the suggestion below of statutory compensation as a part of a direct right of action. An alternative to having the APP entity undertake the mitigating steps is to pay an amount to the individual who has had their privacy interfered with so they can take mitigating steps. The determination route and placing responsibility on the APP entity is likely to be more effective as the APP entity has greater knowledge, or at least access to such knowledge, as to the steps that can be taken. Further economies of scale will result for the APP entity that must deal with all of the effected individuals.

Proposal 25.6

The Report recommends that the Federal Court and the Federal Circuit and Family Court of Australia be given the power to make "any order it sees fit" after a civil penalty provision relating to an interference with privacy has been established.

The courts need to have power to go beyond ordering a civil penalty if the range of impacts of privacy interference are to be appropriately addressed. However, in addition to allowing for "any order it sees fit", the legislation should provide examples of particular orders that may be made. The Report seeks to align the Court's powers under s 13G of the *Privacy Act* dealing with civil penalties and s 55A of the *Privacy Act* where a determination of the OAIC is to be enforced. The power to

make such orders (including a declaration of right) as it thinks fit under s 55A is in the context where the OAIC could address a range of matters that are set out in the Act. The civil penalty provision is much more limited and focuses on penalties only. Examples of the types of orders that may be made in civil penalty proceedings should be specified. Taking the *Corporations Act 2001* (Cth)[20] as an example, see compensation orders (s 1317H), relinquishment orders (s 1317GAB - pay the Commonwealth an amount equal to the benefit derived and detriment avoided because of a contravention of a civil penalty provision) or publication of information orders (s 1324B) and the orders specified in s 1325.

Proposals 25.7 and 25.8

Insufficient resources, including personnel, can mean that contraventions are not detected, or if detected are not pursued, or if pursued are resolved without the sanction of a court due to the cost involved.[21] Sufficient funding for a regulator is crucial to the Australian public having an effective regulator in the privacy space.

Proposal 26 A Direct Right of Action

Proposal 26.1

We support a direct right of action for individuals, or groups of individuals through a representative proceeding or class action, to the courts for relief in relation to interference with the individual's privacy.

However, further consideration should be given to whether the circuitous route contained in the design elements put forward by the Report should be followed. In particular:

> (d) The claimant would first need to make a complaint to the OAIC and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme;
>
> (e) Where the IC or an EDR is satisfied there is no reasonable likelihood that the complaint will be resolved by conciliation or the IC decides a complaint is unsuitable for conciliation, the complainant would have the option to pursue the matter further in court;
>
> (f) In cases where the IC has decided that a complaint is unsuitable for conciliation on the basis that the complaint does not involve an interference with privacy or is frivolous or vexatious, the complainant should be required to seek leave of the court to bring an application in the court.

Individuals through the use of a class action, have shown themselves willing to side-step the current procedure under the *Privacy Act* which requires a complaint to the OAIC.

In *Evans v Health Administration Corporation* [2019] NSWSC 1781[22] a class action was filed in the Supreme Court of New South Wales on behalf of ambulance employees and contractors whose sensitive health and personal information was allegedly disclosed by the first defendant (Health

[20] *Corporations Act 2001* (Cth).

[21] Michael Legg, Olivia Dixon and Stephen Speirs, 'Corporate Misconduct & White-Collar Crime in Australia' (Thomson Reuters, 2022) 48.

[22] *Evans v Health Administration Corporation* [2019] NSWSC 1781.

Administration Corporation) to the second defendant (Mr Malik) in 2013. The disclosure was alleged to be: a breach of the Information Protection Principles contained in Pt 2, Div 1 of the *Privacy and Personal Information Act 1998* (NSW); a breach of the Health Privacy Principles in Sch 1, ss 5(1)(c) and 5(1)(d) of the *Health Records and Information Privacy Act 2002* (NSW); a breach of confidence in equity; misuse of confidential information in equity; and/or a breach of the individual's Employment Agreement (being a breach of a term of trust and confidence implied by law and an express and/or implied term of confidentiality); contravention of the *Competition and Consumer Act 2010* (Cth), Sch 2 – Australian Consumer Law, ss 18 and 29; and a breach of the tort of invasion of privacy for which it is alleged the first defendant is liable or vicariously liable.

The causes of action pleaded were claims for:

1) a breach of confidence (and misuse of confidential information) in equity for which the first defendant is said to be liable or vicariously liable;
2) a breach of the individuals' Employment Agreements, through a breach of the term of trust and confidence implied by law; and an express and/or implied term of confidentiality;
3) a contravention of ss 18 or 29 of Sch 2 of the Australian Consumer Law; and
4) a breach of the tort of invasion of privacy, for which the first defendant is said to be liable or vicariously liable.

The relief sought against the first defendant included: damages for breach of contract; damages pursuant to s 236 of the Australian Consumer Law; damages and/or equitable compensation (including aggravated damages) for breach of confidence; aggravated and exemplary damages.

The proceedings settled, and consistent with the class action requirement that settlement must be approved by a court, Ward CJ in Eq found that the settlement was fair and reasonable in the interests of group members as a whole, having regard to the risks associated with the proceedings, including the need to establish novel causes of action.

Evans v Health Administration Corporation suggests that a number of causes of action, other than the privacy action, can be brought to obtain compensation where a person's privacy is contravened. Claims based on breach of confidence, breach of contract and misleading or deceptive conduct may mean that direct action already exists for individuals without needing to engage with the OAIC and its procedures under the Privacy Act. As the class action settled it cannot be said that these causes of action are clearly effective in addressing privacy breaches. Similarly, if the more novel tort of invasion of privacy was to be recognized then this would add a further source of direct action.

In 2022, law firms investigated class actions in relation to the Medibank and Optus data breaches. In both instances a representative complaint was made to the OAIC for a breach of the *Privacy Act 1988* (Cth). The OAIC has commenced investigations into the personal information handling practices of Medibank and Optus in relation to each entities notifiable data breach. However, in early 2023 a Federal Court of Australia class action was commenced against Medibank adopting a similar approach to *Evans v Health Administration Corporation*.[23] Consequently Medibank is at the time of writing subject to competing claims in the OAIC and the Federal Court for the same conduct.

[23] Sam Matthews, 'Medibank class action to test whether data breach claims "worth the candle"' *Lawyerly*, (Web Page, 10 February 2023) < https://www.lawyerly.com.au/medibank-class-action-to-test-whether-data-breach-claims-worth-the-candle/>.

The discussion about a direct right of action does not address situations where the same underlying conduct is pursued through causes of action not in the Privacy Act and not within the purview of the OAIC. This gives rise to a question for the legislature as to how, if at all, it addresses the co-existence of two routes to compensation for privacy contraventions.

One approach would be to take no action. It would most likely then fall to a defendant, such as Medibank, to seek to stay the court proceedings until the OAIC had completed its response to a complaint.[24] It is an abuse of process for a person to sue the same entity twice for the same contravention. In the Medibank example, the underlying conduct is the same, but the legal claims relied on are different. Issues may also arise in relation to avoiding double recovery by plaintiffs. Further, if the non-Privacy Act path was more attractive then individuals would pursue it and go straight to the Federal Court. No grounds for stay would arise and the OAIC would have no role.

The legislature could mandate that no cause of action in relation to a breach of privacy can be brought until the alleged breach has been pursued through the Privacy Act procedure. The OAIC would have a first right of resolution and if it were unsuccessful or inappropriate then another action could be pursued. This is an extension of the proposed design principles above. This prompts the question as to why a government regulator should perform this role. One response is that it offers an opportunity for a more informal and cheaper resolution of a privacy contravention than usually possible through litigation.

Alternatively standing could be given to individuals to pursue claims based on the causes of action in the *Privacy Act* without a role for the OAIC (other than intervention). An individual could bring a claim combining some or all of the causes of action used in *Evans v Health Administration Corporation* and under the *Privacy Act*. This would offer a more streamlined approach to compensation, but would reduce the role for the OAIC.

The Report also puts forward as a design element: Loss or damage must be established and it must have been caused by a privacy interference by an APP entity.

This submission raises for consideration whether a direct right of action should also provide for a minimum amount of statutory compensation where an individual's privacy has been interfered with by an APP entity. A larger sum, equivalent to the actual loss suffered, would be available if loss and causation were proved.

The aim of statutory compensation is to quickly compensate individuals for the inconvenience and minor losses suffered by a privacy breach, such as changing passwords, monitoring bank accounts etc., for which it is not viable to commence legal proceedings, or indeed, complain to the OAIC. Individuals are not left out-of-pocket for these costs. Payments can be readily calculated and paid to the person without the need for litigation. Equally, awarding a small amount of compensation for these losses will provide an incentive for APP entities to prevent a privacy breach. However, the payment of statutory compensation should not prevent an individual who has suffered greater loss, such as when the information disclosed leads to the incurring of financial debts or obligations.

[24] Sam Matthews, 'Medibank foreshadows stay bid as second class action looms' *Lawyerly* (Web Page, 16 February 2023) < https://www.lawyerly.com.au/medibank-foreshadows-stay-bid-as-second-class-action-looms/>.

Three examples of statutory compensation from the United States are:

- *Stored Communications Act of 1986*, 18 U.S.C. § 2707(c). For violations of electronic privacy, plaintiffs may sue for actual damages suffered and any profits made by the violator, subject to a floor of $1,000;
- *Telephone Consumer Protection Act of 1991* (also known as the Junk Fax Act), 47 U.S.C. § 227(b)(3)(B). For violations of the Act's prohibitions of unsolicited advertisements by telephone, cell phone, or fax machine, plaintiffs may seek actual monetary loss or $500 per violation, whichever is greater;
- *Cable Privacy Act* (amending the Cable Communications Policy Act of 1984), 47 U.S.C. § 551(f)(2)(A). For violations of privacy and disclosure requirements by cable service providers, plaintiffs may obtain liquidated damages of $100 for each day of violation or $1,000, whichever is higher.

We do not recommend that the exact US approaches be adopted in Australia. Rather a bespoke statutory compensation model could be added to the *Privacy Act* to address compensation for minor losses and encourage compliance.

Proposal 28 Notifiable Data Breaches (NDB)

The report discusses our earlier submission, rejecting our suggestion about the serious harm threshold. The challenge we raised earlier is that the entity making the decision will not have sufficient information to know whether "serious harm" might result to some individuals caught up in a data breach. Data breaches affect differently placed individuals differently – whereas some people may not be concerned about a leak of information that might previously have appeared in a phone book (such as physical address), others do have reason to be concerned (eg if they are a victim survivor of family and domestic violence).

The report gives three reasons for rejecting our suggestion for reform in this area, being:

- The fact that "it is expected that entities will err on the side of caution and notify unless they can demonstrate, for example, that the information subject to an eligible data breach was encrypted and therefore the likelihood of harm was low.";
- Notification fatigue and "unnecessary distress" if people receive notification of data breaches that they should not need to be concerned about;
- Compliance burden.

In response to the first of these, we would suggest that rather than relying on unwritten "expectations", it would be preferable to build this into the wording of the legislation. In other words, to require notification unless it can be demonstrated that the likelihood of serious harm is low. There is no reason to have legislative wording that does not align with what the government expects organisations to do. If information is (properly) encrypted, then disclosure would not be required even under the test we propose as the entity would be in a position to conclude that the risk of serious harm is low (and thus meet a reversed onus).

In response to the second of these, it would be useful to have more data on the extent to which disclosures would increase and point at which "fatigue" may set in. It is paternalistic to assume that people would rather not be informed because of a "too much information" problem. This also

ignores the extent to which communications can be tailored to the level of risk, for example a recommendation to those affected to take urgent action versus language that suggests that only those in vulnerable circumstances should be concerned. There is also the possibility in lower risk situations of relying on alternative means of notification (such as in customer newsletters, website notifications, a central searchable repository) where that is in line with the urgency of the risk. What is unacceptable is a situation where individuals cannot discover, even if they are diligent, that their data is involved in breach.

In response to the third of these, the regulatory burden associated with additional notification could itself provide an incentive for stronger security measures *ex ante*. In other words, the more the costs of data breach can be internalised within the organisation with the ability to implement stronger security measures, the more cyber security investments organisations will make, which benefits those (natural persons) who rely on them.

The data notification scheme is important because it promotes the transparency that is essential for justified public confidence in how organisations manage their data. Transparency also enhances cyber security as publicity is a strong motivation to minimise the risk of a breach. We thus believe the changes we propose will ultimately benefit not only data subjects (particularly vulnerable ones), but also cyber security practices across organisations.

Proposal 29.3 Harmonisation

We support this proposal for all key issues, particularly around fair and reasonable processing requirements, reforms to the definitions of 'personal information' and 'consent', data breach notification, protection of children and vulnerable people, automated decision-making, targeting and profiling and security, retention and destruction.

Hub members have recently undertaken research[25] in relation to 'regulatory overlap' (or a lack of harmonisation) in the case of cyber security obligations in certain critical infrastructure sectors. We have identified several broad instances of overlap. While such regulatory overlap has the potential to cause harm, the literature indicates that in a Federal system some overlap is likely inevitable. However, opportunities for coordination and collaboration between stakeholders are also likely to mitigate harm. This would need to be a continuing process as attempts at harmonisation of regulation may be successful at one point in time, but nevertheless become 'disconnected' or 'deharmonised' due to the complexities of a federal system. As part of our research, we have recommended the creation of a forum for collaboration and coordination between cyber regulators (Cyber-Reg), following and building on the models of examples already operating such as the Digital Platforms Regulators Forum or the Council of Australian Financial Regulators.

[25] Susanne Lloyd-Jones, Kayleen Manwaring, Tyrone Berger, Rob Nicholls, Lyria Bennett Moses 'Complex Regimes: Mapping Australia's Cyber Security Regulatory Landscape for Cloud Services' (forthcoming); Susanne Lloyd-Jones and Kayleen Manwaring, 'Complex Regimes – Regulatory Overlap in the Cloud' (2023, Working Paper). Copies of these can be provided on request, dependent on permission from our funding providers.

A Cyber-Reg forum would encourage sharing of expertise, capability and identify potential gaps, cross-over and information asymmetries and could ask relevant questions such as:

- To what extent are there functional advantages in involving multiple agencies?
- How can each regulator's expertise be harnessed to advance cyber security uplifts in specific areas?
- What regulatory activities best fit with expertise and existing jurisdiction?

Yours sincerely,

Lyria Bennett Moses

Michael Legg

Kayleen Manwaring

Megha Uppal