Centre for
Artifical Intelligence
and Digital Ethics

Response to the Review of the *Privacy Act 1988* Issues Paper

Centre for AI and Digital Ethics and Melbourne Law School
November 2020

Executive Summary

The Centre for Artificial Intelligence and Digital Ethics (CAIDE) and Melbourne Law School are delighted to provide this submission to the Attorney General's Department review into the *Privacy Act*. Our response does not address all questions raised in the Issues Paper, but rather focuses on key issues and concerns based upon the expertise at CAIDE and Melbourne Law School.

There have been significant advances in digital technology since 1988 when the *Privacy Act* was introduced. The rate of change has seen the emergence of new tools for business and society and an intensification of increasingly data-driven businesses practices. A review of the *Privacy Act 1988* is timely in order to address concerns about the collection, storage and use of data and personal information in Australia. The ACCC's *Digital Platform Inquiry* highlighted a number of challenges being brought about by the dominant presence of digital platforms in data driven consumer transactions and increasing role that processing personal information has for the economy.[1]

While the scope of the issues paper is focused upon the *Privacy Act*, this is an opportune time to think more broadly about Australia's privacy, data protection and use frameworks. There are various initiatives being led by government, some driven from the Productivity Commission's Inquiry into *Data Availability and Use*.[2] These include the Data Availability and Transparency Bill[3] and Consumer Data Right.[4] Taking a wide approach to the scope of reform would ensure harmonisation and complementarity across the various regimes governing the use and disclosure of personal information.

We hope these insights help to inform the privacy and data protection landscape in Australia, from socio-technical, legal and ethical perspectives.

For more information, please contact Professor Jeannie Paterson, Co-Director CAIDE on jeanniep@unimelb.edu.au.

[1] ACCC, *Digital Platforms Inquiry Final Report* (July 2019)

[2] Productivity Commission (2017) *Data Availability and Use,* <https://www.pc.gov.au/inquiries/completed/data-access>

[3] Office of the National Data Commissioner, *New Legislation* (Web Site) <https://www.datacommissioner.gov.au/data-sharing/legislation>.

[4] *Competition and Consumer Act 2010* - Part IVD — Consumer Data Right.

AI and data intensive industries

The proliferation of data, coupled with improvements in computer capability and the ability to transmit data across the globe, are powering new products, applications and services. The use of data and personal information has been a key driver of economic growth. Underpinning this growth has been the use of advanced analytical practices and algorithms to better understand peoples' desires and preferences to offer increasingly tailored solutions.[5] Australian privacy law needs to address the use of personal information as training data for algorithms and automated decision making.

Training data

One of the key challenges is how to govern the use of personal information as it is used as training data for various models.

Aggregate and longitudinal datasets, often containing personal information, are used in the training of machine learning models. What safeguards should be in place for the use of such data, especially if the resultant algorithms are going to be inform automated decision-making processes? Should there be a limit on these ancillary uses of personal information that is publicly available? Should such a restriction apply to all secondary uses or should there be permitted use scenarios, such as research?

Data that is available for public access can be scraped and analysed to better identify people, build richer profiles and support the training of machine learning and other systems. Should personal information disclosed in a public forum be able to be scraped and reused? If so, should both businesses and consumers be able to make use of this information? Most websites prohibit the scraping of their data, limiting consumers' ability to undertake price monitoring or comparison. However, the same sites often use consumers' data for profiling. A recent example is Facebook's challenging the Ad Observer browser extension developed by New York University.[6] Individuals consent to providing Ad Observer with access to their Facebook data to better understand the targeting of political advertising.[7] Facebook argues that this is against the terms of use of their platform, reflecting the power imbalance between commercial and consumer interests. Scraping may also raise specific IP issues; often personal information is collected from public forums and used to support the development of machine learning algorithms. What, if any, safeguards should be made available in relation to the use of publicly available personal information?

Both identified and de-identified data of varying quality can be bought through data brokers and exchanges. These use cases are novel and evolving and are often not contemplated by individuals, or even the collectors, when they initially consent to the collection of data. While often the consent process will afford the collector a broad degree of latitude, there are emerging use cases that require greater analysis to ensure appropriate safeguards. An example is Clearview AI scraping photo data from the web to train their facial recognition algorithms.[8]

[5] The most common application is targeted advertising.

[6] Rebecca Heilweil 'Facebook glitch blocks certain political ads, raising new questions about transparency' *Vox* (online, 30 October 2020) <https://www.vox.com/recode/2020/10/30/21540443/facebook-political-ad-targeting-transparency-nyu-browser-extension>.

[7] *Ad Observer* (Web Page) <https://adobserver.org>.

[8] Louise Matsakis 'Scraping the Web Is a Powerful Tool. Clearview AI Abused It' *Wired* (online, 25 January 2020) <https://www.wired.com/story/clearview-ai-scraping-web/>.

Automated decision making

Another trend that is arising is the use of digital technologies to automate decision making. This is occurring across a range of contexts in government and the private sector, such as to assess credit scores[9] or provide tailored pricing based upon individual preferences.[10] The use of automated decision making based upon data from the individual is complex. Often the algorithms used are 'black boxes' with privacy notices providing limited transparency as to their operation such as what data factored into a decision. They also have limited explainability where they do not provide a clear explanation about how the decision was arrived at by the automated system. Transparency and explainability are important considerations when designing automated systems as they build trust and can ensure that personal information is used in a responsible manner. Transparency and explainability are essential to ensure the contestability of any automated decisions.

In order to ensure that automated decision making does not unfairly impact users of systems, safeguards need to be in place to ensure that: only appropriate data is used for the decision; there is informed consent from the consumer for these processes to occur; and there is an opportunity for redress as appropriate to the potential harm. The Australian Government's AI Ethics Principles provide a number of principles to guide the development of AI systems, including transparency, explainability and contestability.[11] Compliance with the law needs to also be front and centre as the speed and scale of automated decision-making can cause irreparable harm.

Personal information

The definition of personal information in the *Privacy Act* is from a time when the lines between public and private data were clear. With advances in technology, seemingly benign behaviour – the keystrokes we use, the word patterns we generate, the data 'detritus' that can be correlated – may identify us as individuals. Further, devices that deliberately capture and use our data have increased in our daily lives. Our smart watches and rings, voice activated speakers, programs that track our eye movement for engagement all gather and collate data. Advances in computer power have made it easier for large data sets to be analysed where information that is allegedly 'de-identified' or 'anonymised' could identify an individual. For example, upon the release of de-identified public transport ticketing data by the Department of Transport in Victoria it was discovered that individuals could be identified.[12] The same happened with the release of a subset of Medicare's MBS records.[13]

What needs to be contemplated is the privacy of individuals as well as groups. Incomplete and ambiguous definitions, as well as poor applications of de-identification techniques, can lead to data being claimed as de-identified, when in fact it still contains personal information.[14]

It follows that at least some allegedly de-identified data should comply with the protections of the *Privacy Act*. All data that is categorised as de-identified needs to be treated with caution under the assumption that

[9] Frank Pasquale, *The Black Box Society* (Harvard University Press, 2015).

[10] Choice recently revealed that the dating service Tinder uses personal data to provide different prices to different groups of people, Saimi Jeong *Tinder charges older people more* (Web Page, 11 August 2020) <https://www.choice.com.au/tinderprices>.

[11] 'AI Ethics Principles', *Department of Industry, Science, Energy and Resources*, (Web Page) <https://www.industry.gov.au/data-and-publications/buildingaustralias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles>.

[12] Chris Culnane, Benjamin I P Rubinstein and Vanessa Teague 'Stop the Open Data Bus, We Want to Get Off' (2019) arXiv <https://arxiv.org/abs/1908.05004>.

[13] Chris Culnane, Benjamin I P Rubinstein and Vanessa Teague 'Health Data in an Open World' (2017) arXiv <https://arxiv.org/abs/1712.05627>.

[14] Chris Culnane and Kobi Leins 'Misconceptions in Privacy Protection and Regulation' (2020) 36 *Law in Context* 36 1.

the *Privacy Act* still applies unless it is unequivocally demonstrated it does not – i.e. reidentification is not reasonably possible considering current technologies, practices and capabilities.[15]

Careful attention needs to be paid to the increasing practical and technical capacity to link sources of otherwise benign information, which may provide a profile of sensitive and personal (and most importantly, identifiable information). Anonymisation should not be assumed to produce data sets that do not contain personal information.[16] The definitions of 'personal information' includes reasonably identifiable information, while 'de-identified' encompasses reasonability in relation to being able to identify an individual. The application of reasonableness in relation to de-identification should reflect the current computing capacity to reidentify individuals and link to other information, with the onus to be placed on the entity de-identifying the data.

In addition to reviewing the adequacy of threshold tests of identifiability, there is a need to consider other components of the definition of 'personal information'. In particular, the requirement that data be 'about' an individual may be usefully revised in light of the material scope of the European Union's General Data Protection Regulation (GDPR).[17] The GDPR prefers the term 'relate to' which invites consideration of a broader range of material relations between data and persons beyond the individual as subject matter.

Collection

Digital technologies have enabled the collection and transmission of greater volumes of personal information from a variety of devices. The principle of data-minimisation in Australian Privacy Principle 3 needs to be strengthened to ensure that only information that is clearly relevant for the provision of the service or product is permitted (with higher standards for sensitive information as per APP 3.3 and 3.4). The collection of personal information should align to a clear purpose and use case. Where a greater volume of data is collected than required, organisations should seek to minimise its impact, for example by processing data on devices closer to the user as opposed to in the cloud to reduce data flow and subsequently transmitting recorded and de-identified aggregate results.

Exemptions

The exemptions, such as for employee records and small business, should be removed to the extent they impact the ability to comply with the objectives of the Act, which is 'to make provision to protect the privacy of individuals, and for related purposes'[18] and to operate with other regimes. For example, the employee record and small business exemptions impose severe restrictions on the Act's operation and have historically been part of the reason why Australia has not been assessed as adequate in its compliance with European data protection standards. Further, exceptions to these exemptions have been found both as a matter of case law in *Lee v Superior Wood Pty Ltd*[19] regarding the employee records exemption, and in the statute with ss 6D(4)(b) & (c) relating to health information, and disclosures made 'for a benefit, service or

[15] Ibid.

[16] Office of the Victorian Information Commissioner, *Disclosure of myki travel information: Investigation under section 8C(2)(e) of the Privacy and Data Protection Act 2014 (Vic)* <https://ovic.vic.gov.au/wp-content/uploads/2019/08/Report-of-investigation_disclosure-of-myki-travel-information.pdf>, where the release of a dataset by the State Government of Victoria containing 'anonymised' data was found to include identifiable information.

[17] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1.

[18] *Privacy Act 1988* s 2A.

[19] [2019] FWCFB 2946.

advantage' under the small business exemption. This means that their full scope of application is very uncertain.

As opposed to relying upon exemptions, collection and use should have a clear basis. For example, the GDPR has a strong focus upon consent and has several defined bases for the collection and processing of personal data. For instance, the performance of a contract, or that there is public interest, or that the data controller has a legitimate interest. While not advocating for direct transcription of the GDPR, an Australian regime that sets a high bar for protection, balanced with appropriate and legitimate-use cases, would strike a balance between protection and use. The starting premise should be the minimisation and protection of personal information, followed by putting the onus on the APP entity to establish how such collection and use is authorised (such as through consent).

Small business

The small business exception raises particular concerns, as it places a large portion of the Australian economy outside the scope of the Act. The risks of this approach have recently been laid bare by the fact that COVID19-related tracing and tracking is required by many small businesses to enter or purchase goods – with no obligation to keep the data collected safe and private (apart from obligations under the common law and under statutory standards that might apply outside the *Privacy Act*). Online accounting software, websites to manage digital transactions and payments and now digital check-in systems involve the capture of personal information and are most often provided by third-party vendors. There is a risk that this data might be stored in an insecure manner, and open to access from nefarious actors and other third parties.

The removal of the small business exemption would ensure that small business is attuned to the need to appropriately collect, use and dispose of personal information obtained within the course of their business.

Empowering information self-determination

The Act should aim to empower individuals to manage their personal information. Digital technologies are making this increasingly complex as the data being recorded may not be directly obtained from the individual. For example, the use of web tracking technologies to profile consumers to target advertising is one area, raised in detail in the *Digital Platforms Inquiry*.[20]

In order to support the goal of informational self-determination, especially in the digital context, CAIDE accepts that mechanisms for notice informed consent play and important role in assisting people themselves to manage their privacy. In this section, we identify some of the challenges that arise in relation to effective information self-determination in the digital context. Primarily these arise from the limits to genuinely informed consent in the collection of personal data, and the limited efficacy of notices in proving consumers with control over the collection and processing of their personal data.

An additional complexity is added through the aggregation and collection of data from third parties. For example, when an individual enters into a relationship with an organisation, it is very likely that the organisation is going to need to collect some personal information. Where the process becomes opaque is where data is transferred to third parties to be combined with other data sets for analysis or aggregated for commercial gain. Such transfers need protection of the data use by the third parties, whereby the collecting agency could be deemed liable for any breaches of the privacy performed by an entity that they transferred data too. Additionally, robust de-identification is necessary to ensure that individuals cannot be re-identified. This is likely to reduce the level of granularity of the level of analysis available. However, the use

[20] ACCC, *Digital Platforms Inquiry Final Report* (July 2019).

of advanced techniques such as differential privacy, or the creation of synthetic data could retain a greater level of granularity. Collectors need to continue having some responsibility for the personal information they collect after de-identification and disclosure.

Notice

The provision of notice is an important part of informing people about what data is collected, how it is used and who it might be disclosed to. As noted in the Issues Paper many privacy notices are long and complex and it is understood that many people do not read the lengthy legal documents.[21] Even where consumers read the accompanying documents, they may struggle accurately to assess the future risks arising from the disclosure of personal information. This limitation arises from the inevitable 'bounded rationality of individual decision making and assessments of future risks and harms, particularly those that are not monetised or concrete, as with privacy harms.[22]

Compounding this is the lack of recourse available for privacy notices. While the *Australian Consumer Law* protects against unfair contract terms,[23] the operation of the provision requires a contract to be in existence.[24] While the provision of personal information is often framed as something to be traded in exchange for a free service, it is unclear whether a contract would arise in all circumstances.[25] One option to improve the notice regime would be to ensure that privacy notices are subject to the same kind of rules prohibiting unfair contracts.

Additionally, many digital devices collect personal, and sensitive, information from people without a clear mechanism to provide a collection notice. This is prevalent in digital technologies, such as IoT devices that can capture data that could reasonably identify an individual passively in a public space. Sometimes these devices do not have the option to display notice to users given their design limitations, for example without a screen.

To better protect individual privacy, CAIDE recommends a standard format for privacy notices that will allow consumers to develop expertise in reviewing and understanding the scope of collection policies. Such standards should be framed around 'privacy by design' principles, such as only collecting the information needed for basic functionality. For additional uses or greater functionality, there should be requirements for consumers to consent to such use. The form and content of the notices should be as clear and simple as possible, noting the target audience. The use of infographics, labels and the active use of technologies such as dashboards could greatly support consumers in their decision-making about personal information and improve the capacity for meaningful consent about data collection and use.[26]

Requirements for privacy policy notices should of course be complemented by substantive rules, including limits on practices that are not fair or inconsistent with individuals' reasonable expectations. For example, one area of limitation, requiring a specific opt in policy, should be on the disclosure of data to third parties that does not pertain to the primary purpose for collection.

---

[21] Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (2020) 23(1) *Information, Communication & Society* 128.

[22] Caroline Beaton, 'Humans Are Bad at Predicting Futures That Don't Benefit Them' *Atlantic* (Online, 2 November 2017), https://www.theatlantic.com/science/archive/2017/11/humans-are-bad-atpredicting-futures-that-dont-benefit-them/544709/.

[23] *Australian Consumer Law* ss 23–28.

[24] Damian Clifford and Jeannie Paterson, 'Consumer Privacy and Consent: Reform in the Light of Contract and Consumer Protection Law' (2020) 94 *Australian Law Journal* 741, 750.

[25] Ibid.

[26] The use of technology to support consent was recommended by the ACCC in the *Digital Platforms Inquiry*. For further discussion see Jeannie Paterson, Suelette Dreyfus and Shanton Chang *What We See and What We Don't: Protecting Choice for Online Consumers Policy Report* (2020, University of Melbourne), forthcoming.

Consent

Consent to collection, use and disclosure of personal information

Consent has an important role in supporting information self-determination. Consent empowers individuals to make decisions and exercise autonomy about the disclosure and use of their personal information. While consent is a primary requirement, it should not be the only aspect relied upon. The process of consent needs to be supported by good design and technologies to allow individuals genuinely to manage risk and exercise choice, and as noted above substantive safeguards on unfair or unreasonable data use or conduct inconsistent with individuals' reasonable expectations of such use.

Consent should be seen as one element among a suite of protections. This is due to the problematic nature of consent in light of existing online agreements, including their inaccessibility and length,[27] the lack of power of to negotiate different terms and conditions,[28] bundling of consents to include uses of data that are not strictly necessary to deliver the relevant good or service, and the linking of different sources of information to be reflected back to the consumer. Australia needs new standards for consumers to have a real choice and have agency, through the privacy standards, about what they want to accept from providers. Some of these solutions may be technical, but the regulatory frameworks need to reward and require these technical options for consumers. One example could be to use technology to empower consumers to manage their privacy for online services by entering their privacy preferences on their device that would then communicate those preferences to be applied automatically upon access.[29] Enabling such an approach needs to be safe by default and enforceable to ensure managing privacy is easy for consumers.

A hypothetical about obtaining an estimate on car insurance is illustrative. A consumer could provide basic information about the type of car and where it is parked. This minimum information would allow the insurance algorithm to return a price. Alternatively, an individual may wish to provide greater information to provide a more accurate picture. As such, they should consent to providing additional personal information, such as their location history while driving, to improving the data available to the algorithm to calculate a quote for a premium.

Existing protections need to base themselves on the principle of data minimisation and safeguards. Individuals face a difficult time accurately modelling future risks.[30] For consent to be effective the purpose and use of collection needs to be clearly articulated and understood by users. One of the areas worth expanding in detail in the forthcoming Discussion Paper is the relationship between the individual and the organisation that collects personal information. This relationship between the parties should be the foundation of the consent to give and use the personal information provided.

Disclosure of personal information to third parties

In our opinion, one difficulty with consent is the disclosure of personal information to third parties. There are a variety of third parties to whom information could be disclosed for various purposes. Often this is consented to through cleverly crafted documents that allow data to be shared broadly to third parties. While acceptable there needs to be a distinction between the various kinds of sharing based upon the degree of risk. There is a need to differentiate between organisations providing a service to the data controller, and the data controller profiting off or from the disclosure of personal data. For example, a bank hosting its customer data on Amazon Web Services and a bank selling insights of customer profiles based upon de-

[27] Obar and Oeldorf-Hirsch (n 21).

[28] Jeannie Paterson, Suelette Dreyfus and Shanton Chang, *What We See and What We Don't: Protecting Choice for Online Consumers Policy Report* (2020, University of Melbourne), forthcoming.

[29] This may overcome the complex site-by-site approach taken in the EU.

[30] Beaton, (n 22).

identified data to businesses.[31] Organisations holding personal information should be required to demonstrate that the data was legitimately obtained, for example by providing details about data provenance.

However, clear notification should be required when de-identification of data and the use and disclosure of data that has been extracted from personal information occurs. Establishing a regime around this is complex but individuals should be able to know where their personal information is shared and consent to these disclosures on a case-by-case basis. Entities that share data should remain partly responsible to ensure that consumers do not have to find where their personal information has ended up. This could include partial responsibility for breaches of shared data, whether direct or through re-identification. Such a mechanism would encourage greater diligence on behalf of organisations sharing data.

Stronger protections should be put in place when there is a change of data custodian. Consent should be required to transfer the custody of personal information to a new organisation, with the deletion of data being the default. This would limit companies becoming data targets through takeovers.

Withdrawal of consent, objection, and erasure

Any regime based upon consent also needs to accommodate the withdrawal of that consent and subsequent erasure of data. Failure to include such steps reduces the importance of consent as it limits individual freedom.

Consent once granted for a specified purpose should remain until that purpose is no longer applicable – i.e., the processing changes, or an individual withdraws their consent. Updating consent should normally occur only when new uses of personal information arise. Regularly updating privacy policies and terms and conditions feeds into consent fatigue. If usage details are updated, should individuals be required to consent to updated terms to continue using the product or service?

Erasure should be introduced into the *Privacy Act* as it will empower citizens in their privacy self-management by allowing them to exercise full control over their data. This aligns with transparency (knowing what data is available) and correction (being able to amend the data). We note that there might be some limiting factors for the erasure of some data – for example, when an individual still wishes to transact with the company holding the data.

Where consent does not provide the legal justification for the collection, use or disclosure of personal information, the relevance of a data subject explicitly notifying a data custodian that they object to the processing is in doubt. A right to object, similar to that contained within the GDPR,[32] should be considered for inclusion within the *Privacy Act*. This does not provide an individual with a veto over appropriate processing. It does, however, limit continued processing in the face of an explicit objection to be justified.

In addition to the ability to object or request erasure of personal information there should be limits on the duration organisations can hold personal information. This would provide a safeguard for individuals. Certain events should trigger default retention, restriction and deletion rules. For example, when an individual ends their relationship with an entity their personal information should be retained for a specified time period with restrictions on the use of the data in that time period before being deleted.

Information should be retained securely for a specified time period, such as in line with various limitation of actions statutes. Should the data be retained it should have additional safeguards imposed limiting

[31] The data would need to be appropriately de-identified. See discussion of personal information above.

[32] *General Data Protection Regulation*, Article 21.

disclosure and use. If the entity seeks to de-identify the data, this needs to be done in a robust manner to prevent re-identification.

Defaults and minimum standards

A greater focus needs to be placed on building privacy into technology. The *Privacy Act* should be amended to require minimum standards that would provide a baseline for privacy protection and guide developers to incorporate privacy into the design and development of systems.

When such requests become egregious and unfair considering the nature of the product or service, and/or the sophistication of the parties, then there is requirement for greater regulation to prohibit unfair terms.[33]

Ensuring fairness alone is not sufficient more needs to be done to make sure the onus does not fall totally on consumers. CAIDE recommends that options for users should be pro-privacy by default. The reason is that many people simply accept the default rules, often due to consent fatigue. By setting minimum collection, use and disclosure standards, individuals can then actively make the decision to open access to their personal information for additional use cases.

Alongside these minimum settings the process of notice and consent should be standardised as much as possible to provide clarity and consistency to consumers. The use of technology can support consumers in understanding and managing their consents. Already dashboards are being developed to support management of data under the *Consumer Data Right*, which could provide a solid foundation to extend across other domains.

Prohibitions of some acts and practices need to be considered to avoid unintended consequences. In the digital context, it is the collection of personal information into vast datasets that create a higher level of privacy risk.

Transparency

Transparency ensures that individuals know what data is being collected along with how it is being held, used, and disclosed. Transparency is one of the core pillars of privacy protection as it supports individuals to have knowledge and awareness about their data and provide meaningful and informed consent to the collection, use and disclosure.

Transparency needs to be a core feature with organisations providing individuals with a clear way to see what data is collected, how it is used and to whom it is disclosed.

Use

Use should focus on how the collecting entity seeks to use the data and in what manner. The intended use goes to the heart of the purpose for collection. The advent of digital technologies is creating a wide range of use cases that are becoming increasingly automated. Clearly articulating the use of the data is important so that individuals can understand how their data is being used. Use of advanced algorithms, AI and machine learning techniques requires organisations to invest in improving the transparency and explainability of these systems so that individuals can better understand how their data is being used and processed, and decisions about use are arrived at.

[33] Damian Clifford and Jeannie Paterson (n 24).

The requirement that use of such technologies be 'fair' should be extended and strengthened to provide individuals with remedy in circumstances where data is not used consistent with reasonable expectations.

Another area of concern is profiling of individuals through the collection and aggregation of various data sources. Should the creation of profiles that combine multiple data sources about an individual be restricted? It is likely that such profiles should be treated as sensitive information, given the wealth of insights often obtainable from this information such as race, political opinions or sexual orientation.

Disclosure

Disclosure should be separated from use. This is due to use of data by the collecting organisation being different from disclosure. Often disclosures are benign – for example, writing personal information into specific software supplied by a vendor. At other times there are greater risks when multiple data sets are shared and aggregated. Combining personal information from multiple sources can allow organisations to obtain greater insights about their customers.

However, these combinations often reveal more about the individual than the analysis of an organisation's personal data. Such disclosures are often consented to by individuals as part of privacy notices, so we believe that greater protections need to be placed upon the disclosure, or obtaining, of data for the purposes of aggregation and analysis. While some organisations may seek to gain insights through the disclosure of de-identified data, CAIDE recommends that given the capability of reidentification of personal information from de-identified datasets (given enough additional information), robust safeguards need to be designed to ensure that the information is de-identified in such a manner as to prevent re-identification.

A global market for digital products and services

Australia operates in a global marketplace for digital products and services. Most of our digital services are provided by foreign companies. The *Digital Platforms Inquiry* highlighted the market power held by Google and Facebook in search and social media respectively.[34]

Emerging technologies are increasingly global in nature – both as imports to Australia and for Australian companies providing digital protects to an international market. The realities of cross-border products and services means that Australian companies must comply with various international privacy and data protection regimes. Seeking harmonisation would reduce the regulatory burden on organisations and provide consistency across jurisdictions.

CAIDE recommends that the forthcoming Discussion Paper explore the economic realities of the digital economy to outline the various options to improve alignment with both the GDPR and regional regulatory regimes.

We caution about designing a regime that does not align Australia to global trends in privacy and data protection as this would increase the compliance costs for organisations. For example, many organisations handle their data in a manner that is GDPR compliant.

[34] ACCC, *Digital Platforms Inquiry Final Report* (July 2019).

Enforcement

Powers under the Privacy Act and role of the OAIC

The current enforcement regimes are underequipped to address the evolving importance that data and personal information has to the economy. This could be due to the lack of resourcing on the part of the regulator – but also goes to the design of the regime, which puts the regulator at the heart of the matter both as the initial finder of fact but also as the entity that can bring a representative action. Establishment of a data ombudsman is one avenue to increase capacity to address complaints and resolve disputes relating to personal information.[35]

Given the centrality of data to the provision of a wide range of services to society and government, the enforcement regime should be expanded to align with other protective regimes. For example, the *Competition and Consumer Act 2010* and *Australian Consumer Law* provide a suite of enforcement options for the regulator and for individuals. Adding this flexibility would provide greater power to the Commissioner to bring an action against a data custodian, while also allowing a direct right of action to be brought by individuals. A direct right can also be beneficial where large privacy breaches occur, enabling claims to be brought together as a class action. Such an approach would ensure multiple actors are able to scrutinise and enforce privacy provisions, as opposed to just the Commissioner with the aim of improving compliance with the legislation.

Statutory tort

The common law has developed in the United Kingdom[36] and New Zealand[37] to recognise a tort for invasion of privacy, evolving from breach of confidence. Australian law has not yet followed suit, despite the court leaving open such a possibility in *Lenah Game Meats*.[38] The law may develop to provide an action for a tort of invasion of privacy, but one limiting factor is the need for the right case to emerge and be litigated to the apex court.

The tort of invasion of privacy would complement the existing actions and provide some coverage for those instances where there may not have been a direct relationship between the person providing the personal information and the processor. Additionally, the introduction of a statutory tort could provide greater certainty about what remedies might be available following a breach of privacy.

Some serious invasions of privacy might be so egregious as to involve criminal sanction. This should be available as a deterrent to the more egregious behaviours. There will be overlap with existing criminal laws and should focus on the more egregious abuses of personal information such as obtaining data illegally, hacking or unwarranted surveillance, or the non-consensual disclosure of highly sensitive information including intimate partner images.

CAIDE recommends that the starting point of analysis be the Australian Law Reform Commission's 2014 proposal for a statutory tort outlined in their S*erious Invasions of Privacy in the Digital Era* report.[39]

---

[35] Such a proposal was recommended by the ACCC in the *Digital Platforms Inquiry* (Recommendation 23).

[36] *PJS v News Group Newspapers Ltd* [2016] UKSC 26.

[37] *Hosking v Runting* [2004] NZCA 34.

[38] *ABC v Lenah Game Meats* (2001) 208 CLR 199.

[39] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (2014, ALRC Report 123) - <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/>.

Interaction with other regulatory schemes

The *Privacy Act* should provide comprehensive protection for the handling and use of personal information, there might be some specific risks and concerns that are not be appropriate. Activities such as obtaining personal information such as through computer hacking or fraudulent behaviour or disclosing of specific kinds personal information, for example sharing intimate partner images,[40] should continue to be incorporated into the criminal law.

There are a range of similar initiatives occurring relating to personal information and data. The Consumer Data Right and *Data Availability and Transparency Bill* are creating comprehensive regimes to facilitate the disclosure and sharing of data. Care needs to be taken to ensure personal information is handled in an appropriate manner and the treatment of personal information starts from the principles-based approach contained in the *Privacy Act*. In particular there is potential for to build on the complementary regulatory framework between the *Privacy Act* and the *Australian Consumer Law*. The ACL contains a number of 'safety net' provisions such as the prohibition on misleading conduct, unconscionable conduct and unfair contract terms, that can support the intention to ensure genuine protection to individuals provided in the more specifically focused *Privacy Act*. For example, the ACCC has made use of the prohibition on misleading conduct in s 18 of the ACL to hold platforms and other entities to representations about data collection and use. As noted below, reform to improve consent procedures should complement the already robust requirements in the Consumer Data Right regime.

Legislative design

Legislative design is an important part of building an appropriate regulatory regime. CAIDE recommends that the Department focus on how best to achieve harmony and alignment across various pieces of regulation focusing on privacy and data protection. A starting point is to replicate best practices from other legislative regimes. Small differences between overlapping legislation creates complexity and incoherence in the law. It also creates a regulatory burden making it difficult for organisations to comply with their obligations.

Areas such as consent and notice provisions should be aligned across regimes, which would make it easier for businesses to rollout a consistent approach and better for consumers due to the similar requirements. A starting point for consideration is the recently established measures in the *Consumer Data Right*.

[40] *Criminal Code Act 1995 (Cth)* s 474.17A.

About the Centre for AI and Digital Ethics

CAIDE was launched in 2020 to undertake cross-disciplinary research, teaching and leadership on the ethical, regulatory and legal issues relating to AI and digital technologies. The establishment of CAIDE reflects the fact that the emergence of AI and digital technologies are having society-wide impacts and therefore require a broad range of perspectives to balance the technical, social, regulatory and economic factors of technology. CAIDE brings together expertise from engineering, law, arts and science applying a cross-disciplinary perspective to shape our understanding and development of AI and digital technologies.

Privacy and data protection are central considerations in the ethical design and development of digital technologies. CAIDE has an active research program in this area and has published on privacy, ethical design and regulation of digital technologies. CAIDE has recently commenced a project exploring regulatory mechanisms for protecting reasonable expectations of privacy: the roles of consent and fairness in Australian and Indian Data Protection Law in partnership with Jindal Global University.

The Centre also has an active teaching program offering courses in digital ethics at the undergraduate, postgraduate and professional levels.

https://law.unimelb.edu.au/centres/caide

Contributors

Prepared by **Adam Lodders**, Academic and Research Programs Manager, Centre for AI and Digital Ethics

With contributions from:

Karin Clark, Senior Fellow, Melbourne Law School

Dr Chris Culnane, Honorary Fellow, School of Computing and Information Systems

Kobi Leins, Senior Research Fellow in Digital Ethics, School of Computing and Information Systems

Prof Jeannie Paterson, Co-Director Centre for AI and Digital Ethics

A/Prof Mark Taylor, Melbourne Law School

Prof Megan Richardson, Melbourne Law School

Thank you to Julia Paterson for editing assistance.