NATIONAL ARCHIVES OF AUSTRALIA

# Review of the Privacy Act 1988

## NATIONAL ARCHIVES OF AUSTRALIA

4 DECEMBER 2020

RKS R1188342020

# Contents

# 1. EXECUTIVE SUMMARY

***About the National Archives***

The National Archives of Australia (National Archives), established under the *Archives Act 1983* (Archives Act), provides leadership in best practice management of the official record of the Commonwealth and ensures that Australian Government information of enduring significance is secured, preserved and available to government agencies, researchers and the community.

The National Archives:

- sets information management requirements for Australian Government agencies
- ensures the Australian Government creates and keeps records of its actions and decisions to demonstrate accountability to the community and evidence the integrity of the operations of the Australian Public Service
- authorises disposal of information assets with no ongoing value to government or community
- selects and preserves the most significant records of the Australian Government
- makes these records available to government and community as a national resource to enrich and inform how we live today, and into the future.

It provides advice and assurance that the Australian Government has access to authentic, reliable and usable Commonwealth records to enable evidence-based decisions, provide sound advice, develop good policy and deliver programs effectively and, to facilitate access to the archival resources of the Commonwealth.

Community members need to be confident that the information they share with government will be held securely, shared responsibly and made available as accurate proof of their entitlements when needed. Good information management is essential to building trust in the creation, collection and use of Australian Government information as documentary heritage, to meet the outcomes required by government and community.

The National Archives understands that well-managed government records are foundational to the Australian Government's digital transformation and innovation agenda, to deliver world-leading digital services, as well as the future cultural identity and economic prosperity of the nation. It is a national resource for knowledge creation and sharing, which underpins the integrity of Australia's system of democracy, enabling trusted interactions between the community and a transparent, responsive and accountable government.

***National Archives response to the Terms of Reference***

# 2. DEFINITION OF PERSONAL INFORMATION

The definition of personal information in section 6 of the *Privacy Act 1988* (Privacy Act) is fairly wide. As it stands, the definition could capture information about an individual whose identity might be apparent only when the information is combined with other information not held by an agency. However, as the Attorney-General's Department (AGD) notes in its Issue Paper, more personal information about individuals is being captured and processed as a result of the growing digital economy. Further clarity around what constitutes personal information is necessary to ensure that Australian privacy law continues to maintain relevancy in increasingly complex digital environments.

We note that, pursuant to the definition of 'record' as outlined in the Privacy Act, Commonwealth records within the meaning of the Archives Act that fall within the open access period and/or are within the custody of

the National Archives, are not considered to be personal information, nor do the Australian Privacy Principles (APPs) apply to them. We also note, however, that section 33(1)(g) of the Archives Act exempts a Commonwealth record from public access if it contains "information or matter the disclosure of which under this Act would involve the unreasonable disclosure of information relating to the personal affairs of any person (including a deceased person)". While this does not have the effect of applying the APPs to open access period Commonwealth records, it does make privacy concerns or principles a primary consideration in deciding whether to make the relevant Commonwealth records publicly available.

The National Archives' *Access Examination Policy – personal, business and professional affairs of a person* guides and informs decision-making in considering whether the release of a Commonwealth record containing information about a person would be an unreasonable disclosure of their personal, business or professional affairs. The policy provides a non-exhaustive list of some of the information and material that the National Archives consider relate to personal affairs:

- adoption records
- applications for employment, expressions of interest, recruitment panel assessments, reports or recommendations
- assessments of competency, intellectual capacity
- attempted suicide or details about successful suicide
- character assessments
- detailed or long term medical histories
- documents relating to identity
- domestic matters
- financial information
- illegitimacy
- information given in confidence
- information provided or gathered by Australian Government agencies relating to allegations of a personal nature
- information gathered for intelligence purposes or profiling an individual
- information that would identify victims of atrocities or crimes
- medical conditions
- personnel records of people employed by the Australian Government
- physical characteristics that are not visible and to which a stigma may attach
- sexual relationships and preference
- welfare case files, including those created by defence organisations
- wills that are unlikely to be in the public domain.

The policy outlines the following questions to consider when determining whether the release of the information would be an unreasonable disclosure:

1. What is the nature and perceived sensitivity of the information to be disclosed.
2. What is the age and current relevance of the information – the older the record, the less likelihood that it would be unreasonable to disclose the information.
3. What is the age of the subject of the information. Or if the subject is deceased, what is the age of their descendants.
4. To what extent is the information already in the public domain.
5. Does the information have a credible source.
6. Are there cultural factors that should be considered.

In *Colakovski v Australian Telecommunications Corporation* (1991) 29 FCR 429 the Federal Court considered the meaning of "relating to…personal affairs" in s 41(1) of the *Freedom of Information Act 1982*.

In summary, they considered that "personal affairs":

- cannot be defined in a definitive way
- refers only to the affairs of a natural person and not to the affairs of a corporation
- refers to information which concerns or affects the person as an individual, whether it is known to other persons or not
- may, in some circumstances, include information relating to a person's vocation, work performance or capacity.

In considering "unreasonable disclosure" Lockhart J said in this case (at 438):

*What is "unreasonable" disclosure of information for purposes of s 41(1) [of the FOI Act] must have as its core public interest considerations. The exemptions necessary for the protection of "personal affairs" (s 41) and "business or professional affairs" (s 43) are themselves, in my opinion, public interest considerations. That is to say, it is not in the public interest that the personal or business or professional affairs of persons are necessarily to be disclosed on applications for access to documents. The exemption from disclosure of such information is not to protect private rights, rather it is in furtherance of the public interest that information of this kind is excepted from the general right of public access provided the other conditions mentioned in sections 41 and 43 are satisfied.*

Heerey J referred to a different aspect of the public interest test (at 441):

*Turning to the criterion of unreasonableness ... it seems to me that attention is directed, amongst other things, to whether or not the proposed disclosure would serve the public interest purpose of the legislation, which is to open to public access information about government which government holds, this being information which in truth is held on behalf of the public. I do not think it is necessary in order to make out the [exemption] that there is some particular unfairness, embarrassment or hardship which would endure to a person by reason of the disclosure. Such matters, if present, would doubtless weigh in favour of exclusion. But if the information disclosed were of no demonstrable relevance to the affairs of government and was likely to do no more than excite or satisfy the curiosity of people about the person whose personal affairs were disclosed, I think disclosure would be unreasonable*.

As such, the application of s 33(1)(g) of the Archives Act goes beyond the mere identification of 'personal affairs' or what under other circumstances may be considered personal information, but rather concerns whether or not release would have an unreasonable adverse effect on the person.

Because of this additional test, and that Commonwealth records released for public access by the National Archives are at least 20 years old and have been found following assessment to not be an exempt record, the National Archives submits that the distinction of Commonwealth records under the Archives Act from the operation of the Privacy Act and the APPs should continue.

Technical information

The National Archives is supportive of the inclusion of technical data such as unique on-line identifiers in the definition of personal information. The National Archives would further recommend that this technical information be managed as would any other information, from creation to disposal. We look forward to providing more detailed views on this issue as this review progresses.

Protection of inferred personal information

Personal information drawn from digital platforms or data analytics can lead to concerning inferences about individuals. For instance, protected attributes or sensitive personal information such as sexual orientation, race, political opinions, health information and so forth can be inferred from major internet platforms which are now routinely utilised by federal government departments and agencies (APP entities). To that end, protection of inferred personal information is a key consideration of current privacy law reform.

The difficulty with introducing a legal protection of inferred personal information lies in the fundamental questions of how, why and for what purpose data is processed and, crucially, at what point inferences become personal information that require protection by law. Such a protection will need to address, for example, when inferring sexual orientation, political opinions or health/mental health, is 'socially acceptable or overly privacy invasive and under which circumstances'.[1]

Regarding inferences revealing personal information, the National Archives recommends that, if the definition of personal information is amended to include interferences, the definition needs to be 'tight', and also provide definitions for "inferences" or "inferences drawn", so that there is no ambiguity regarding whether "inferences derived from other pieces of personal information are considered themselves to be personal information…"[2]

Finally, where government creates or collects inferred personal information it should be managed as would any other information.

Additional protection for de-identified pseudonymised information

As AGD has stated in the Issues Paper, with advances in technology, de-identified data may become susceptible to re-identification. This clearly poses a problem for APP entities seeking to comply with APP 2.

In addition, as technology advances, the ability to predict the text in redacted documents may reach the point where additional protections currently used may not work.

Information about deceased individuals

While we acknowledge s 33(1)(g) does apply to deceased persons, as is acknowledged in the Issues Paper, we should note the *Access Examination Policy – personal business and professional affairs of a person* outlines that the potential for unreasonable disclosure of information about a deceased person is low. In some cases it may be appropriate to exempt from release information about a deceased person on the basis that disclosure would be unreasonable because of the effect on descendants. The following formula may be used by the National Archives:

1. date or approximate date of birth of subject known – assume descendants still alive up to 130 years from that date
2. date or approximate date of birth of subject unknown – assume descendants still alive up to 110 years from date of documents or date of incident

[1] Wachter, S and Mittelstadt, B "A right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI" (2018) Oxford Business Law Blog: https://www.law.ox.ac.uk/business-law-blog/blog/2018/10/right-reasonable-inferences-re-thinking-data-protection-law-age-big

[2] Blanke, J.M., "Protection for 'Inferences Drawn:' A Comparison between the General Data Protection Rule and the California Consumer Privacy Act" (2020), https://ssrn.com/abstract=3518164

3. if it is known or can be assumed that the subject was a young adult (under 30 years), middle-aged (in their 40s or older at the time of the incident, this information should be used to approximate his or her date of birth for the purpose of the above calculations.

We would caution any statements in this review that could infer that the National Archives often, or as a general rule, exempts Commonwealth records with information about a deceased person. Indeed, with the passage of time the release of many of these documents would no longer be considered unreasonable, and there is often a compelling public interest in making these records available to preserve individual, community and the nation's memory. By example it was reported in 2014 revelations from records of World War I servicemen that a number had contracted sexually transmitted diseases in transit to the fronts. While we acknowledge this information may have caused embarrassment to their descendants, it has provided a wider context on the impacts of World War I on ANZAC servicemen that has been explored further by historians and academics, which would not have been possible if we were to apply s 33(1)(g) of the Archives Act to these documents.

# 3. ERASURE OF PERSONAL INFORMATION OR 'THE RIGHT TO BE FORGOTTEN'

## 3.1. Should there be greater requirements to destroy or de-identify personal information held by entities

The introduction of a requirement to destroy or de-identify information held by entities could introduce a significant a regulatory burden for APP entities, particularly those that are small, such as the National Archives and risks the destruction of evidence that impacts on the rights and entitlements of Australians now and in the future. It may also have an adverse impact on the ability to conduct historical research on matters that document the interaction of Australians with their government.

Although fees to erase personal data could be introduced, this may only go some way to managing the administration of numerous requests to erase data. The extent to which information should be destroyed needs to be considered in the context of personal information having additional uses, for example evidential use in legal proceedings, future research and so forth.

Any destruction or de-identification should be managed so that information of national significance or public interest that will continue to have value to the Australian Government and the community for generations to come, is retained in accordance with the Archives Act.

This includes information that relates to:

- government authority, action and accountability
- identity, interaction and rights and entitlements
- knowledge and community memory.

The National Archives notes there have been numerous instances of records providing an invaluable insight into Commonwealth and Australian memory, despite the records containing personal and sensitive personal information that could theoretically be subject to a right of erasure were it to be implemented. Examples highlighted from the National Archives' current record retention notices and disposal freezes include:

- Royal Commission into Aged Care Quality and Safety
- the protection and detention of children in the Northern Territory
- violence, abuse, neglect and exploitation of people with disability

- allegations of abuse in Defence
- the Vietnam war.

All of the above records by its nature involve personal information about individuals, including sensitive information, yet their unqualified destruction would cause irreparable harm to Commonwealth memory, truth telling, and preserving the rights of individuals over the passage of time. While we do not suggest these records should necessarily be public from the moment of creation, nor made available without sufficient caveats or clarified secondary records, their complete erasure and hence inability to be made subject to an open access period within the meaning of the Archives Act would also be a significant loss.

## 3.2. Should a right of erasure be introduced? If so what should be the key features if such a right? What would be the financial impact on entities?

If large volumes of individuals request the erasure of personal information, a significant regulatory burden could be introduced. Consideration to the extent to which data can be erased needs to be considered. The range of interactions with entities may range from a simple service transaction through to information that may be crucial evidence in a future court case. As such the exclusion of some types of data should be considered with any introduction of a right of 'erasure'.

When considering the right to erasure of information created, received or used by Australian Government agencies which are Commonwealth records under the Archives Act, the functions and the powers of the National Archives under the Archives Act need to be considered. As indicated above, under sections 3C and 24 of the Archives Act, the National Archives has the power to determine archival resources of the Commonwealth for permanent preservation and gives Australian Government agencies permissions for disposal of temporary-value Commonwealth records, unless such disposal is required by any other law. These permissions are given in the form of records authorities issued to agencies (https://www.naa.gov.au/information-management/records-authorities). Section 26 of the Archives Act prohibits any alterations to Commonwealth records that are more than 15 years old without the National Archives' permission with the exception of instances when required by any law.

In addition, the National Archives occasionally withdraws its disposal permissions to support the work of Royal Commissions, Inquiries and other government processes which deal with high-risk and high profile issues in the Australian society. Information about such instances are available on our corporate website (https://www.naa.gov.au/information-management/disposing-information/disposal-freezes-and-retention-notices). As indicated above, this includes records related to aged care quality and safety; institutional responses to child sexual abuse; protection and detention of children in the Northern Territory; all of which are in the public interest in being preserved and made available to Royal Commissions and other investigations.

Any proposed right to erasure of personal information needs to be balanced with the requirements of the Archives Act and the powers of the National Archives. Personal information worthy of permanent preservation should be safeguarded by government agencies until it can be transferred into the National Archives collection.

The approach under the Europen Union General Data Protection Regulation (GDPR) limits the erasure of personal data which only applies in certain circumstances. The following data types can be excluded:

- The data is being used to exercise the right of freedom of expression and information.
- The data is being used to comply with a legal ruling or obligation.

- The data is being used to perform a task that is being carried out in the public interest or when exercising an organisation's official authority.
- The data being processed is necessary for public health purposes and serves in the public interest.
- The data being processed is necessary to perform preventative or occupational medicine. This only applies when the data is being processed by a health professional who is subject to a legal obligation of professional secrecy.
- The data represents important information that serves the public interest, scientific research, historical research, or statistical purposes and where erasure of the data would likely to impair or halt progress towards the achievement that was the goal of the processing.[3]
- The data is being used for the establishment of a legal defence or in the exercise of other legal claims.

Any amendments to the Privacy Act would need to ensure that evidentiary data that may be needed for future use is not erased. For example, information that constitutes Commonwealth records under the Archives Act and that supports ongoing Australian Government business or relates to the National Archives selection principles (https://www.naa.gov.au/information-management/disposing-information/transferring-information/transferring-information-national-archives/how-we-select-national-archives):

- government authority, action and accountability
- identity, interaction and rights and entitlements
- knowledge and community memory.

This also applies to any Government data that relates to disposal freezes issued under the Archives Act.

# 4. OTHER MATTERS

## 4.1. Interaction between the Privacy Act and other regulatory schemes

The National Archives does not support greater harmonisation of privacy protections under the Archives Act and the Privacy Act. The privacy protections in the Archives Act work well and are specifically tailored to address the types of personal information collected by the Australian Government and released for public access under the Archives Act, following assessment once they reach the open access period.

# 5. CONCLUSION

In summary, the National Archives makes the following key recommendations:

1. The exemption of open access period records for the purposes of the Archives Act, from the personal information provisions of the Privacy Act, should continue.
2. Any insertion of a right to erasure should be balanced with the requirements of the Archives Act and the powers of the National Archives to ensure that personal information worthy of permanent preservation is protected by government agencies until it can be transferred into the National Archives collection.
3. The National Archives does not support greater harmonisation of privacy protections under the Archives Act and the Privacy Act. The current differences reflect the different purpose of each Act, including the age of documents released under the Archives Act for public access.

[3] https://gdpr.eu/right-to-be-forgotten/