Receiving Officer
DATActReview@finance.gov.au
Department of Finance
1 Canberra Ave
Forrest ACT 2603

Electronic Frontiers Australia Inc.
ABN: 35 050 159 188
W: [redacted]
E: [redacted]

By email

21 May 2025

Dear Receiving Officer,

RE: Statutory Review of the Data Availability and Transparency Act 2022 (Cth) ("DAT Act") - Issues Paper

EFA welcomes the opportunity to provide commentary on the Statutory Review of the DAT Act Issues Paper.

EFA's submission is contained in the following pages.

We would welcome the opportunity to provide further commentary if required.

About EFA

Established in January 1994, EFA is a national, membership-based, not-for-profit organisation representing Internet users concerned with digital freedoms and rights.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political, and civil liberties issues involved in the use of digital communications systems.

Yours sincerely,

John Pane
Chair
Electronic Frontiers Australia

Introduction

While it has been several years since the introduction of the DAT Act, fundamental digital rights continue to be violated and cause harm to millions of Australians every year. EFA remains concerned by the government's active overriding of existing privacy legislation by creating an inherently unsafe data sharing framework that operates in parallel to existing laws.

The DAT Act has essentially created a "back door" mechanism for accessing data that would otherwise be protected from access and that was provided to government on the assumption that it would be so protected. The DAT Act effectively overrides protections provided for sensitive and other personal data, such as that collected about individuals by the Census. While there may be a "public interest test" for the sharing of this data, the evaluation is not transparent to the public nor does it properly include a transparent accounting for human rights, civil liberties and privacy rights .

Unlike all similar nations, Australia lacks a federal enforceable human rights framework that contains both privacy and data protection provisions for its citizens. The DAT Act further undermines Australians' right to privacy and to have their data protected from unauthorised access, use and disclosure.

In a time of increasing threats to data security and privacy driven by significant advancements in computing power and technology, EFA again asks, among other recommendations, that the government fast track a federally enforceable human rights framework which contains both privacy and data protection provisions, to fast track Tranche II of Privacy Act reform package as a matter of urgency, and to replace the "5 Safes Framework" with a more robust, safe and trustworthy security methodology.

Summary of Recommendations

1. **EFA recommends** that Australia adopts a robust, federally enforceable human rights framework that contains privacy and data protections reflecting today's extensive technological and computing capabilities and the pervasive surveillance based, data extraction model they enable.
2. **EFA recommends** that pending the introduction of a robust, federally enforceable human rights framework, the DAT Act be amended to require the prior completion of a Human Rights Impact Assessment by the Office of the National Data Commissioner as part of its data sharing use case assessment process.
3. **EFA recommends** that the DAT Act be amended to specifically include a public interest test for data sharing requests that is compatible with balancing the competing needs of government and civil society with a focus on evaluating human rights, civil liberties and privacy impacts.

4. **EFA recommends** that the DAT Act be amended at Sections 138 requiring the National Data Commissioner to publish on its web site anonymised case notes concerning all complaints received by the agency and further, that Section 102(2) be amended to make it a mandatory requirement for the National Data Commissioner to publish on its web site the findings of investigations made under Sections 99 and 101.

5. **EFA recommends** that Section 45 of the DAT Act be amended to facilitate the transfer of the specific oversight powers of regulation and enforcement to the Office of the Information Commissioner. The National Data Commissioner should concentrate on advocacy, education, and advice.

6. **EFA recommends** that: (1) Tranche II of the the Privacy Act reform package be fast tracked urgently, and, as part of that review, (2) The definitions of "personal information"[1] and "de-identified information[2] as proposed By Salinger Privacy in their submission on the Review of the Privacy Act Issues Paper be adopted.

7. **EFA recommends** that for the purposes of transparency and accountability, the Office of the National Data Commissioner publishes on its web site the list of recommended standards, methods and techniques it recommends or requires for data de-identification purposes in support of an entity's participation in the DATA Scheme.

8. **EFA recommends** that use of the Five Safes/Data Sharing Principles approach be abandoned and that it should be replaced with a more robust risk management framework developed in consultation with privacy and risk management experts.

9. **EFA recommends** that Section 88 and 94 of the DAT Act be amended to include both class and representative actions being recognised as protected actions and remedies.

10. **EFA recommends** that Australia passes an AI Act modelled on EU principles with strong, independent regulatory oversight supported by a judicial review process.

EFA'S Review and Commentary on the DAT Act 2022

Missing Human Rights Protections

EFA's ongoing analysis of the DAT Act again raises questions about the federal government's full compliance with internationally recognised human rights standards, particularly concerning the fundamental right to privacy. International human rights law, as enshrined in documents such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, clearly establishes the right of every individual to protection against arbitrary or unlawful interference with their privacy[3].

[1] https://www.salingerprivacy.com.au/wp-content/uploads/2020/11/20-11-20_Privacy-Act-review_Salinger-Privacy_Submission.pdf , pg 5.
[2] Ibid, pg 7
3 https://www.icj.org/wp-content/uploads/2022/05/Digital-Technologies-and-Human-Rights-Briefing-Paper-FINAL-VERSION-May-2022.pdf

The DAT Act's power to facilitate the broad sharing of government-held data, especially when considering the identified weaknesses in its privacy protection mechanisms specified below, creates concerns about its compatibility with this core human right. Its primary emphasis on enhancing data availability, without the presence of sufficiently robust privacy safeguards and explicit data subject rights, falls short of meeting the standards set out in international human rights law regarding the protection of privacy. International legal frameworks typically require that any interference with an individual's right to privacy must be both necessary and proportionate to the achievement of a legitimate aim. The broad data sharing powers granted under the DAT Act, and the potential for unintended consequences, continues to fall short assessed against these established criteria.

Government data shared under the DAT Act may contain sensitive information about vulnerable groups within the population, including victims of domestic violence, immigrants, First Nations people, LGTBQIA+ people, and people with disability. The use of this data, particularly in the development of government policies or the delivery of services, carries the potential for discriminatory outcomes if not handled with extreme care and consideration[4]. Notably, the DAT Act does not explicitly address the potential for algorithmic bias or discrimination that could arise from the analysis and use of shared data in automated decision-making processes[5].

To better align with human rights principles, the DAT Act needs to incorporate specific provisions designed to safeguard against any discriminatory impacts on vulnerable groups that might result from the sharing and subsequent use of government data[6]. This should include requirements for comprehensive human rights impact assessments to identify potential risks and the establishment of mechanisms to proactively detect and mitigate any algorithmic bias that could lead to unfair or discriminatory outcomes. Ensuring that the use of shared data upholds the principle of non-discrimination is a critical aspect of aligning the DAT Act with fundamental human rights standards.

Australia is unique among western liberal democracies in that it does not have a robust federally enforceable human rights framework that could underpin the DAT Act and ensure individuals are provided with certain baseline protections. As a consequence, the passage of the DAT Act has removed existing protections without providing robust additional ones in exchange.

EFA recommends that Australia adopts a robust, federally enforceable human rights framework that contains privacy and data protections that reflect today's extensive technological and computing capabilities and the pervasive surveillance based, data extraction model they enable.

EFA recommends that pending the introduction of a robust, federally enforceable human rights framework that the DAT Act be amended to require the prior completion of a Human Rights Impact Assessment by the Office of the National Data Commissioner as part of its data sharing use case assessment process. An exemplar template can be found here: https://policy-practice.oxfam.org/resources/human-rights-impact-assessment-framework-621501/

4 https://nzccl.org.nz/briefing-on-the-data-and-statistics-bill/

5 https://onlinelibrary.wiley.com/doi/full/10.1002/ajs4.342

6 https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities

Civil Liberties Concerns

The DAT Act raises several concerns regarding its potential impact on fundamental civil liberties. There is continuing, and well founded apprehension, about the possibility of government overreach and the misuse of shared data, potentially leading to consequences similar to the "robodebt" scheme, but in an accelerated form. While the Act explicitly states that data cannot be shared for law enforcement or national security purposes, the broad data sharing powers granted for other purposes could still indirectly affect civil liberties. This could occur if the shared data is used in ways that result in discriminatory outcomes or lead to undue surveillance of individuals or groups.

The DAT Act facilitates the creation of extensive datasets that can be accessed by multiple government entities and public Australian universities. This increased interconnectedness of data held by various bodies amplifies the potential for dataveillance, where the aggregation and analysis of seemingly disparate pieces of information can be used to create detailed profiles of individuals and their activities. Even if the data is initially de-identified, the ability to link it with other datasets will erode anonymity and enable more intrusive forms of monitoring, potentially undermining the fundamental right to privacy and potentially creating a chilling effect on freedom of expression and association,[7] as well as putting vulnerable groups at risk of harm.".

The DAT Act stipulates that data sharing must be for a purpose that serves the public interest. While this principle is fundamental to justifying the sharing of public sector data, EFA holds ongoing concerns about the term "public interest" and the potential for inconsistent application of this test. A lack of clarity in what constitutes "public interest" in different contexts leads to both inconsistent or bad decisions and a lack of transparency in the decision-making process for data sharing projects.

The DAT Act further provides that data sharing projects must be reasonably expected to serve the “public interest”. However, as noted above this term is inadequate, is highly subjective and is silent on the weighing of the benefits to the government against our fundamental human rights, liberties and privacy. To ensure that this justification for data sharing does not become overly broad and infringe upon our fundamental human rights, liberties and privacy, the DAT Act should include a clear and specific definition of "public interest" in this broader and balanced context. Furthermore, establishing mechanisms for independent oversight of data sharing projects would be crucial to ensure that the claimed public benefit genuinely outweighs any potential negative impacts on civil liberties and that a proper balance is maintained between these competing interests.

EFA recommends that the DAT Act be amended to include a public interest test for data sharing requests that is compatible with balancing the competing needs of government and civil society with a particular focus on human rights, civil liberties and privacy.

Regulatory Transparency and Accountability

While the DAT Act introduces measures such as a public register of data sharing agreements and establishes the role of a National Data Commissioner, EFA has strong concerns regarding the level of detail in transparency provisions and the effectiveness of accountability frameworks.

[7] https://www.sciencedirect.com/science/article/pii/S1071581923001295

Specifically, EFA notes the continuing weaknesses relating to the broad discretion of data custodians, the inadequacy of penalties for non-compliance, and the limited avenues for direct recourse for individuals. Furthermore, the dual role of the National Data Commissioner as both a promoter and regulator of data sharing continues to be an obvious conflict of interest. Addressing these flaws through legislative amendments and clearer guidelines is crucial for building public trust and ensuring the responsible and effective use of shared government data.

While the establishment of a public register is a positive step towards transparency, the effectiveness of this measure hinges on the level of detail mandated for inclusion in the register and its accessibility to various stakeholders. For example, the data sharing agreement titled "Sharing of Disability Services National Minimum Data Set" using data originating from Tasmania to support creation of the National Disability Data Asset[8], lacks sufficient detail about both what data elements were to be shared and how the data elements were to be treated so as to render them "de-identified data".

The DAT Act also mandates that the National Data Commissioner must include information on activities undertaken in relation to their regulatory functions in an Annual Report. This report is intended to provide an overview of the operation of the DATA Scheme, including the Commissioner's activities in accrediting entities, handling complaints, and enforcing compliance.

The effectiveness of the Commissioner's Annual Report as a transparency instrument depends on its scope and level of detail. Whilst the 2023/2024 Annual Report[9] does seem to meet the Commissioner's compliance obligations under Section 138 of the DAT Act, regulatory transparency should be enhanced by the publication of complaint case notes and also the publication of any assessments/audits conducted respectively under Sections 99 and 102 of the DAT Act. Such information can be published on the Office of the National Data Commissioner's website.

EFA recommends that the DAT Act be amended at Sections 138 requiring the the National Data Commissioner to publish on its web site anonymised case notes concerning all complaints received by the agency and further, that Section 102(2) be amended to make it a mandatory requirement for the National Data Commissioner to publish on its web site the findings of investigations made under Sections 99 and 101.

Managing Regulatory Conflict

At the heart of the accountability framework is the National Data Commissioner, an independent statutory office holder responsible for regulating the DATA Scheme. The Commissioner's functions are wide-ranging and include accrediting eligible entities as users or service providers, handling complaints from Scheme participants and the public, and assessing and investigating potential breaches of the Act or data sharing agreements. To support the Commissioner in their role, the Act also establishes the National Data Advisory Council, which provides advice on ethical considerations, the balance between data availability and privacy protection, trust and transparency, technical best practice, and industry and international developments related to data sharing.

8 https://www.datacommissioner.gov.au/node/308

9 https://www.datacommissioner.gov.au/sites/default/files/2024-10/ONDC_Annual%20report_2023-24.pdf

To deconstruct this further the National Data Commissioner has advice related functions under Section 43[10] and guidance related functions under Section 44[11] of the DAT Act. Further, at Section 45[12] of the DAT Act, the National Data Commissioner has regulatory and enforcement powers.

EFA considers it inappropriate for the National Data Commissioner to be tasked with both promoting the sharing and release of data and with regulation and oversight of entities responsible for protecting data. These two objectives are inherently in opposition. Regulation and oversight of the scheme should be performed by a body that is fully independent of a body tasked with promoting greater data sharing. The National Data Commissioner can perform either one of these roles effectively, but not both.

EFA notes that there is already a Commonwealth body with data oversight functions: the Office of the Australian Information Commissioner (OAIC). EFA is also of the view that there should be a separation of powers for the Office of the National Data Commissioner under the DAT Act.

The OAIC already has broad experience in dealing with data privacy and handling of data breaches and has experienced staff familiar with regulatory functions and the complexities of privacy law. Information is data with meaning, and it seems inefficient for the DAT Act to add a second information commissioner, albeit one with reduced meaning.

EFA recommends that Section 45 of the DAT Act be amended and to facilitate the transfer of the specific oversight powers of regulation and enforcement to the Office of the Information Commissioner. The National Data Commissioner should concentrate on advocacy, education and advice.

The Anachronistic Privacy Act 1988 (Cth): Why Current Definitions Fail

Introduction: The Evolving Landscape of Privacy and Data

The ***Privacy ACt 1988 (Cth)*** ("***Privacy Act***") remains a fundamental concern for EFA and other digital rights and civil liberties organizations. It was drafted in the last century when we faced a completely different tech landscape, one which saw the rise of the Information Society and Post-Industrialism. And while modified several times since 1988, the Privacy Act has never kept pace with technological advancements despite being promoted as capable of doing so.

The Privacy Act was enacted to foster and safeguard the privacy of individuals by establishing regulations for the handling of personal information by Australian Government agencies and subsequently, organisations exceeding a specific annual turnover. This legislative framework, however, was conceived in an era characterised by technological capabilities and data handling practices that bear little resemblance to the complexities of the contemporary digital world. The intervening decades have witnessed a profound transformation in the way information is generated, disseminated, and used, primarily driven by the proliferation of the internet, the advent of big data, the scalability of cloud computing, data analytics, and the burgeoning field of artificial

[10] https://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/daata2022312/s43.html
[11] https://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/daata2022312/s44.html
[12] https://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/daata2022312/s45.html

intelligence. This technological evolution has catalysed the emergence of a pervasive surveillance based, data-driven economy, where personal and other data has become a highly valued and actively traded commodity.

The initial objectives of the Privacy Act, while commendable at the time of its enactment - **39 years ago** - did not anticipate the sheer scale and the intricate sophistication of present-day data processing technologies. The core challenge lies in the legislative inertia of the Privacy Act by adopting a principle of technological neutrality in the face of relentless and exponential technological progress. This has resulted in a widening chasm between the protections afforded by the law and the actual privacy vulnerabilities encountered by individuals. Furthermore, the ascendance of the surveillance-based data economy has created powerful incentives for the extensive collection and multifaceted exploitation of personal data, further highlighting the inadequacy of the existing legal framework to provide meaningful safeguards and remedies.

Important Definitional Terms in the Privacy Act

In this evolving landscape, the definitions of "personal information"[13] and "de-identified information"[14] enshrined within the Privacy Act, which have remained largely static since their inception, are now seriously flawed and patently anachronistic[15]. Current definitions struggle to adequately capture the intricacies and potential risks inherent in modern data handling methodologies, thereby rendering the Privacy Act increasingly inadequate for its fundamental purpose of protecting individual privacy in the digital age[16].

The Problem With the Definition of "Personal Information"

Section 6(1) of the Privacy Act currently defines personal information as "information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not". While this definition may appear comprehensive at first glance, its application in the context of the digital age reveals significant limitations in its ability to encompass the full spectrum of data that can impact an individual's privacy.

The Privacy Act's emphasis on information being "about" an identified or reasonably identifiable person often overlooks the reality that in the digital sphere, individuals can be subjected to targeted advertising, detailed profiling, and consequential actions based on data that does not explicitly reveal their identity through conventional means such as names or addresses. The ability to single out and act upon individuals based on unique identifiers or combinations of seemingly non-identifying data points, a common practice in online environments, patently falls outside the purview of the current definition.

---

[13] https://www.spruson.com/what-is-personal-information-under-the-privacy-act/
14 Ibid.

[15] https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/PrivacyAmendment47/Report/Chapter_2_-_Key_issues

[16] https://www.uts.edu.au/globalassets/sites/default/files/article/downloads/david-lindsay---privacy-act-review_submission.pdf

A significant deficiency in the current definition of personal information lies in its failure to explicitly address modern digital identifiers that are now fundamental to online tracking and profiling. The Act does not specifically mention crucial elements such as Internet Protocol (IP) addresses, device identifiers, geolocation data, online identifiers including cookies, or data inferred through algorithmic analysis. This omission creates a significant ambiguity regarding whether such information falls under the definition of personal information, despite its well-established capacity to identify and meticulously track individuals' online activities and behaviors.

Examining the Risks in the Definition of "De-identified Information"

The Privacy Act stipulates that personal information is considered to be "de-identified" when it undergoes a process of modification such that it is no longer about an identified individual or an individual who is reasonably identifiable. While this definition establishes a principle, the Privacy Act lacks a sufficiently robust or technologically informed framework for defining and validating the process of de-identification in the face of rapidly advancing technology. Similar to the definition of personal information, the concept of "no longer reasonably identifiable" underpinning the definition of de-identified information suffers from a lack of clear and objective standards, particularly when confronted with the increasingly sophisticated techniques for re-identification and data reconstitution that have emerged in recent years.

The relentless pace of technological progress, especially in the domains of data analytics, machine learning, and artificial intelligence, has dramatically lowered the barrier to reconstituting information that was once considered effectively de-identified back into personally identifiable data[17]. The ability to combine seemingly innocuous data points gleaned from disparate sources, often referred to as auxiliary information, can frequently lead to the accurate re-identification of individuals within datasets that were believed to be anonymous[18]. Furthermore, AI and machine learning tools possess an exceptional capacity for discerning subtle patterns and intricate correlations within vast datasets, including those that have undergone de-identification procedures, thereby exponentially elevating the risk of successful re-identification, a phenomenon often referred to as the Mosaic Effect.[19]

The DAT Act's current definition of de-identified information (a cross reference to the definition under the Privacy Act) does not adequately account for the immense power of modern computing and the sophisticated analytical capabilities of AI, lange language platforms and machine learning systems and to analyze and link extensive volumes of data, thereby fundamentally undermining the intended privacy-preserving function of de-identification techniques.

The Privacy Act fails to clearly delineate between these varying levels of de-identification, leading to potential misunderstandings, inconsistencies in practice, and ultimately, inadequate protection for data that is often claimed to be de-identified or anonymous. This lack of precision in the definition of de-identified information and the tools and methods recommended to achieve this data state inadvertently creates a potential loophole that allows organizations to assert that data has been de-identified even when a significant and demonstrable risk of re-identification persists.

[17] https://www.unimelb.edu.au/__data/assets/pdf_file/0020/4070504/Privacy-Act-Review-Issues-Paper.pdf

[18] https://ovic.vic.gov.au/privacy/resources-for-organisations/the-limitations-of-de-identification-protecting-unit-record-level-personal-information/

[19] https://centre.humdata.org/exploring-the-mosaic-effect-on-hdx-datasets/

Several prominent case studies and real-world examples from Australia and internationally vividly illustrate the inherent vulnerabilities of de-identified data in the face of advanced technology. In one notable instance, researchers at the University of Melbourne successfully demonstrated the re-identification of individuals within a publicly released "de-identified" dataset containing historical health data from the Australian Medicare Benefits Scheme (MBS) and the Pharmaceutical Benefits Scheme (PBS). This was achieved by cleverly linking the ostensibly anonymous health records with publicly accessible information about individuals, such as known medical procedures and year of birth. [20] This case starkly highlighted the surprising ease with which seemingly anonymous health-related data could be re-identified, raising serious concerns about the adequacy of current de-identification practices. [21] Similarly, the release of what was claimed to be "de-identified" public transport ticketing data in the state of Victoria also exposed significant vulnerabilities to re-identification through the potential for linkage with other available datasets. [22] While not originating in Australia, the widely cited example of New York City taxi ride data, where anonymized trip records were re-identified by correlating trip timestamps and pick-up and drop-off locations, further underscores the pervasive risk of re-identification in seemingly de-identified datasets. [23]

The above real-world occurrences serve as compelling evidence of the failure of current de-identification methodologies, often guided by the Privacy Act's insufficiently robust definition, to truly de-identified data in an environment characterised by sophisticated analytical capabilities and the widespread availability of auxiliary information and data sets both publicly and privately available. They unequivocally demonstrate that the risk of re-identification is frequently underestimated, with potentially significant consequences for individual privacy.

EFA recommends that: (1) Tranche II of the the Privacy Act reform package be fast tracked urgently, and, as part of that review, and (2) The definitions of “personal information”[24] and “de-identified information[25] , as proposed By Salinger Privacy in their submission on the Review of the Privacy Act Issues Paper, be adopted.

Are Best Practice Methods Consistently Used to De-identify Personal Information?

The choice of the most suitable de-identification method for a given purpose is highly dependent on the specific characteristics of the data being processed, the intended use of the de-identified information, and the level of acceptable risk for re-identification.

The landscape of data de-identification is shaped by a variety of international standards and regulatory guidelines that provide frameworks, principles, and specific requirements for organizations handling personal information. Key standards and guidelines in this area include ISO/IEC 27559, NIST SP 800-188, guidelines issued by the European Data Protection Board (EDPB), and the HIPAA Privacy Rule in the United States.

20 https://www.unimelb.edu.au/newsroom/news/2017/december/research-reveals-de-identified-patient-data-can-be-re-identified

21 https://www.zdnet.com/article/re-identification-possible-with-australian-de-identified-medicare-and-pbs-open-data/

22 https://www.unimelb.edu.au/__data/assets/pdf_file/0020/4070504/Privacy-Act-Review-Issues-Paper.pdf

23 https://www.unimelb.edu.au/__data/assets/pdf_file/0020/4070504/Privacy-Act-Review-Issues-Paper.pdf

24 https://www.salingerprivacy.com.au/wp-content/uploads/2020/11/20-11-20_Privacy-Act-review_Salinger-Privacy_Submission.pdf , pg 5.

25 Ibid, pg 7

It is unclear if the Office of the National Data Commissioner endorses all of these models above or any one of them as an adjunct to the so called "5 Safes Framework" which underpins data sharing arrangements between data custodians and data requestors, or if the 5 Safes Framework is used in isolation. It is further unclear if the National Data Commissioner, as a function of exercising their powers under Sections 43 and 44 of the DAT Act, which particular de-identification techniques or standards are recommended or required by that office for an entity's participation in the DATA Scheme.

EFA recommends that for the purposes of transparency and accountability the Office of the National Data Commissioner publish on its web site the list of recommended standards, methods and techniques it recommends or requires for data de-identification purposes in support of an entity's participation in the DATA Scheme.

Use of the Five Safes Framework

The DAT Act renamed the Five Safes framework[26] as five *data sharing principles*[27] , but a change in label does not change their effect. This framework is not fit-for-purpose.[28] It takes an overly simplistic approach to information and privacy risk management that encourages a checkbox approach to risk assessment and mitigation - it is rudimentary at best. This approach is likely to increase, not reduce, the potential for harm. The approach privileges the interests of governments and their institutions over those of individual citizens and uses poorly-substantiated claims of nebulous future benefits to justify this increased risk of harm.

An examination of the DAT Act reveals inadequacies in its provisions for ensuring the security of shared data. While the DAT Act mentions the need for "appropriate security safeguards" and the "setting principle" mandates that data be shared, collected, and used within an appropriately controlled environment with reasonable security standards, it lacks the specificity of mandatory information security standards, including data e-identification techniques, that accredited entities must strictly adhere to. This ambiguity in security requirements will lead to inconsistent and potentially inadequate security practices across different entities participating in the data sharing scheme. Relying on a principle-based approach to security without clearly defined and enforceable technical requirements will not guarantee a consistently high level of protection for the sensitive government data being shared.

EFA recommends that use of the Five Safes/Data Sharing Principles approach ultimately be abandoned and that it should be replaced with a more robust risk management framework developed in consultation with privacy and risk management experts and civil society groups like EFA and others.

Representative Complaints/Class Actions

EFA remains very concerned that the DAT Act does not contemplate provisions for making a representative complaint or bringing a class action against a DAT Scheme participant of the Office of the National Data Commissioner.

---

[26] Tanvi Desai, Felix Ritchie and Richard Welpton, 'Five Safes: Designing Data Access for Research' [2016] (1601) *Economics Working Paper Series* <https://uwe-repository.worktribe.com/preview/914753/1601.pdf> ('Five Safes').

[27] https://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/daata2022312/s16.html

[28] Chris Culnane, Benjamin IP Rubinstein and David Watts, 'Not Fit for Purpose: A Critical Analysis of the "Five Safes"' [2020] *arXiv:2011.02142 [cs]* <http://arxiv.org/abs/2011.02142> ('Not Fit for Purpose').

Sections 88 and 94 of the DAT Act effectively pre-empts the rights of individuals to gather together as a class to seek remedy for substantial harms suffered as a result of inappropriate data sharing. This deliberate exclusion for bringing a class action is particularly concerning from an accountability perspective, given the *Robodebt* debacle[29] in which a major agency of the government was found to have engaged in systematically unlawful behaviour[30] and repeatedly failed to discontinue this behaviour.[31]

Sections 88 and 94 of the DAT Act as currently drafted gives the appearance that the Australian government is very concerned that inappropriate data sharing *will* occur and that it is seeking to pre-emptively cut off an important way for individuals to counter the power and resources of the government.

This behaviour by the government does not demonstrate trustworthiness to its citizens.

EFA recommends that Section 88 and 94 of the DAT Act be amended to facilitate both class and representative actions being recognised as protected actions and remedies.

The Urgent Case for AI law, an enforcement agency and judicial oversight

Artificial Intelligence (AI) represents a transformative technological advancement with immense potential to reshape economies and societies worldwide. In Australia, AI and automation are projected to contribute up to $600 billion annually to the nation's GDP by 2030, with a rapidly growing AI industry and significant foreign investment in Australian AI technologies[32]

However, the rapid development and deployment of AI systems are significantly outpacing regulatory efforts to govern their application. This creates a profound challenge, as AI introduces complex risks to individuals, society, and the environment that demand careful and proactive governance. The pervasive influence of AI across various sectors, from healthcare to finance, necessitates robust safeguards to prevent unintended and potentially catastrophic consequences.

Recent international developments highlight the federal government's hesitation to finalise its AI regulatory framework. This is happening amid a backdrop of what is a clearly significant and deliberate effort to degrade the importance of AI safety - led by the United States towards a Big Tech/industry friendly approach that is wrapped in the usual tropes of urgency, productivity, innovation, and prosperity. While this news surely makes tech-oligarchs and venture/techno capitalists smile, the rest of us are worried.

Commonwealth agencies are increasingly using AI solutions and processing both personal and de-identified data in the absence of a regulatory and technical standard vacuum. This is the connection between AI, the DAT Act and the DAT Scheme.

---

[29] Luke Henriques-Gomes, 'Robodebt: Government Admits It Will Be Forced to Refund $550m under Botched Scheme', *The Guardian* (online, 26 March 2020) <https://www.theguardian.com/australia-news/2020/mar/27/robodebt-government-admits-it-will-be-forced-to-refund-550m-under-botched-scheme> ('Robodebt').

[30] Luke Henriques-Gomes, 'Robodebt Scandal: Leak Reveals Unlawful Debts Predate 2015 but Government Has No Plans to Pay Back Money', *The Guardian* (online, 30 May 2020) <https://www.theguardian.com/australia-news/2020/may/31/robodebt-scandal-leak-reveals-unlawful-debts-predate-2015-but-government-has-no-plans-to-pay-back-money> ('Robodebt Scandal').

[31] Letecia Luty and Jamie Luxton, '"It Should Not Have Taken so Long": Robodebt Took a Huge Toll – There Must Be Real Accountability | Letecia Luty and Jamie Luxton', *The Guardian* (online, 3 June 2020) <https://www.theguardian.com/australia-news/2020/jun/04/it-should-not-have-taken-so-long-robodebt-took-a-huge-toll-there-must-be-real-accountability> ('"It Should Not Have Taken so Long"').

[32] https://www.industry.gov.au/news/developing-national-ai-capability-plan

This situation highlights a critical tension between the pursuit of innovation and the imperative for public protection. If the primary focus remains on accelerating economic gains without commensurate regulatory development, the risks associated with AI, such as algorithmic bias, mass surveillance, and job displacement, become not only probable but also more severe and entrenched. This creates a crucial window of opportunity for Australia to proactively establish robust safeguards before widespread AI adoption entrenches harmful practices. Conversely, an "innovation-first" mindset that sidelines comprehensive regulation could lead to a reactive rather than preventative regulatory stance, leaving the nation vulnerable.

EFA believes that the development and deployment of AI must be unequivocally grounded in universal human rights, core democratic values, and the foundational principles of the rule of law. Our advocacy is centered on the urgent need for comprehensive, legally binding AI legislation, supported by an independent and skilled regulatory body, and robust judicial oversight. These three pillars are essential safeguards to ensure that AI fosters trust, enhances safety, protects privacy, and upholds human rights for all Australians.

The concept of a human rights-based approach, consistently championed by digital rights organisations, is not merely an abstract ethical consideration; it is a pragmatic necessity for long-term societal stability and economic trust. If AI systems are allowed to cause widespread discrimination, privacy violations, or undermine democratic processes, public trust will inevitably erode. This erosion of trust can lead to public backlash, hindering adoption and ultimately stifling the very innovation policy makers seek. Therefore, proactively protecting rights through legally binding frameworks becomes a foundational element for sustainable AI development and broad societal acceptance, directly linking ethical principles to economic and social resilience.

Without robust oversight, measurable demonstrations of compliance efforts, and the possibility of enforcement or legal liability, AI actors and Big Tech have few incentives to dedicate the necessary time and resources to conform their practices to these frameworks. The ease with which guidance can be ignored or adherence falsely claimed without repercussions significantly undercuts the usefulness and credibility of such voluntary standards. The reliance on purely internal evaluation and accountability procedures, without transparency obligations or outside review, renders these measures largely meaningless and creates no genuine incentive for AI actors or Big Tech to implement them effectively. This approach ultimately erodes public and industry trust in both the frameworks and the institutions promoting them.

The reliance on voluntary frameworks represents a fundamental misdiagnosis of the power dynamics at play in the rapidly evolving tech industry. It assumes good faith and self-correction where immense profit motives and intense competitive pressures have proven themselves, time and again, to override ethical considerations and public welfare. This effectively allows companies to privatize the benefits of AI development while socializing the potential harms, meaning the public bears the brunt of unmitigated risks without adequate legal recourse or preventative measures.

Australia's current reliance on voluntary principles, despite their ethical merit, creates a significant "governance gap." This gap leaves our nation vulnerable to the very harms observed in less regulated jurisdictions, as industry self-regulation has repeatedly proven inadequate when faced with powerful economic incentives and competitive pressures. This absence of binding law also makes Australia susceptible to regulatory capture, where industry influence can shape policy in its favor, undermining public interest.

Australia must move decisively to enacting legally binding, economy-wide legislation for AI, particularly for high-risk applications. This aligns with the comprehensive, risk-based approach seen in leading jurisdictions like the EU, which categorizes AI applications based on risk levels and imposes strict obligations on high-risk systems.

This legislation should include explicit prohibitions on AI systems that are inherently harmful, unreliable, or biased and cannot be adequately mitigated. This includes, but is not limited to, emotion recognition systems, biometric categorization for surveillance, and predictive policing tools that perpetuate discrimination. Mandatory guardrails must require rigorous conformity assessments, independent audits, and public certification for all high-risk AI systems before and during deployment.

By adopting a robust, human rights-based AI regulatory framework, Australia can set a powerful global precedent and significantly influence the development of international standards, particularly given its existing moderate alignment with EU principles. In a fragmented global regulatory landscape marked by inconsistent approaches and the risk of a "race to the bottom," Australia's choice to prioritise robust, rights-based AI law can strategically position us as a trusted partner and a beacon for ethical innovation. This stance can attract businesses and talent that value responsible development over unchecked growth, fostering a unique competitive advantage in the global AI economy.

Without a robust AI regulatory framework (i.e law, not voluntary guidelines), a suitably resourced enforcement agency, and judicial oversight, we as Australians remain incredibly vulnerable to the ongoing erosion of our privacy and data security, increased bias and discrimination, lack of fairness and equity, job displacement and economic inequality, threats to safety and security, weakening of democratic processes, potential environmental harms, and erosion of human autonomy and control.

The choice Australia makes regarding AI regulation is not merely an economic or technological decision, but a defining moment for our nation's societal values and democratic resilience. A failure to enact binding AI law, supported by strong regulatory and judicial institutions, would represent a profound abdication of responsibility by the government. It would allow even more unchecked technological power to reshape society in ways that undermine fundamental human dignity, erode civil liberties, and ultimately imperil the trust and safety of all Australians. The time for voluntary measures has passed; the time for AI law is now.

EFA recommends that Australia passes an AI Act modelled on EU human rights and harm minimization principles supported by strong, independent regulatory oversight and a judicial review process.

End