New South Wales
Council for Civil Liberties

# NSWCCL SUBMISSION

# NSW DEPARTMENT OF CUSTOMER SERVICE

# REVIEW OF THE NSW DATA SHARING (GOVERNMENT SECTOR) ACT 2015.

**29 March 2021**

**About NSW Council for Civil Liberties**

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts, attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

**Contact NSW Council for Civil Liberties**

http://www.nswccl.org.au
office@nswccl.org.au
Correspondence to: PO Box A1386, Sydney South, NSW 1235

The NSW Council for Civil Liberties (NSWCCL) welcomes the opportunity to make a submission to the Department of Customer Service in read to the Review of the NSW *Data Sharing (Government Sector) Act 2015*.

## Introduction

1. The *Data Sharing (Government Sector) Act 2015* (Act) is undergoing its 5-year statutory review. The Act was the first of the Australian States data sharing laws. The review will determine whether the policy objectives of the Act remain valid and whether the terms of the Act remain appropriate.

2. NSWCCL considers that many of the policy objectives and terms of the Act are not valid or appropriate. Within the last 5 years public perceptions of how data should be shared have changed. The Act does not sufficiently acknowledge the interests of individuals in their own data and further that some government sector data is not appropriate for sharing at all.

   NSWCCL has long held concerns over the manner of the use, collection, and storage of personal information of NSW citizens by the NSW government. It is one matter to share information in a safe and controlled manner where a need can be established that outweighs privacy interests, it is quite another to take little care with the information of others and collect and share it because technology exists to allow it.

3. Community discomfort over data sharing, both in the government and private sector, is increasing. The expectations of a majority of Australians are in favour of more privacy protections over their information, not less. In recent times, the Australian public has been subjected to the Cambridge Analytica and Facebook scandals, CensusFail, RoboDebt, re-identification attacks and numerous data breaches".[1] The latest Government survey of Australians' privacy concerns shows 84% of Australians consider it to be a misuse of their information when supplied to an organisation for a specific purpose and then used for another purpose.[2]

4. The Act deals with the sharing of government sector data with the government Data Analytics Centre (DAC) and between other government sector agencies and the privacy and other safeguards that apply to the sharing of that data.

5. The first and foremost object of the Act is "to promote, in a manner that recognises the protection of privacy as an integral component, the management and use of government sector data…" [3] The Act specifies the purposes for which data sharing is permitted, ensuring that the sharing of health or personal information continues to be in

[1] Floreani, S. (22 Oct 2020) The Data-Sharing Dilemma *Salinger Privacy* https://www.salingerprivacy.com.au/2020/10/22/data-sharing-dilemma/

[2] OAIC 2020 Australian Community Attitudes to Privacy Survey https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey/

[3] S 3(a) Act

compliance with the requirements of the privacy legislation, and requiring compliance with data sharing safeguards in connection with data sharing.[4]

6. The Act as drafted is principled based to allow flexibility to adapt to emerging technology, governance and legal requirements. NSWCCL suggests instead that the Act delivers a low level of certainty and clarity and is inadequate in terms of its privacy safeguards. Despite the superficial assurances it operates, in practice, to override normal privacy safeguards of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and other legislation.

**Government Sector Data**

7. "Government sector data means any data that a government sector agency controls",[5] other than data excluded by the regulations. This is an extremely broad catch-all definition. Such data is actually information about NSW citizens held by government agencies, in order to run government programs and services for our benefit. The government and its agencies are the custodians of its citizens data.[6]

8. Data is not all the same. The sharing of non-personal information, though subject to the purpose test, is not protected by other privacy safeguards. Consent for its repurposed use does not seem to be required.

9. Personal information may contain sensitive information including unit record administrative data that has name, date of birth, address or other personal identifiers, medical records, financial information, criminal records, etc. This kind of information should not be in the public domain nor is it appropriate for public access.[7]

10. Personal information, whilst governed by privacy legislation[8], is often aggregated with, or incidental to, non-personal information. The harm to the individual of reidentification becomes greater in those circumstances. Further, sharing of personal information between agencies that is incomplete cross agency data can lead to decisions that are biased and subject to misuse internally (e.g. stalking) and externally (e.g. hacking).

11. There appears to be no requirement, set out in the Act, that personal information be de-identified prior to sharing. De-identification is in any case not a foolproof privacy-enhancing measure.

---

[4] S 3(d) Act
[5] S 4(1) Act
[6] Op.cit Floreani
[7] Andrews, P. (15 October 2019) Open data is fine, but sharing more data won't solve all problems. What you need to do data properly *The Mandarin* https://www.themandarin.com.au/117995-when-people-need-specific-data-for-specific-things-freely-open-sharing-your-data-is-not-as-helpful-as-you-might-think-what-you-need-to-do-to-do-data-properly/
[8] The *Privacy and Personal Information Protection Act 1998* (PPIP Act) establishes controls and obligations on the disclosure of personal information.
The *Health Records and Information Privacy Act 2002* governs the management of health information held by organisations (public sector agencies or a private sector person) that are health service providers or that collect, hold or use health information.

If data containing personal information is to be de-identified, a protocol needs to be evident as to how that de-identification will occur, whether the data may be re-identified, and if so, how it may be re-identified.

**Government Sector Data and the pandemic**

12. The 2019–20 bushfire emergency and COVID 19 pandemic restrictions have dramatically increased Service NSW processes that capture personal information about the activities of individuals. Additionally, as of 1 January 2021, s. 36(3) (a1) of the *Public Health (COVID-19 Restrictions on Gathering and Movement) Order (No 7),* requires people who enter a hospitality venue or hairdressing salon to register their contact details electronically with Service NSW (using the COVID-19 Safe Check-in tool). When the QR code is scanned at a venue, Service NSW will collect the person's name, contact details, time and date of entry and, crucially, location. Collection of this information is mandatory to gain entry. While assurances have been given about deletion of this data after 28 days, it is not clear that this is being audited.

    Opting out of digital interactions, of this kind, is not a realistic option for most people. Balancing interests therefore amounts to having to agree to terms of access or risking the suffering of economic disadvantage, discrimination, or social exclusion. Community sentiment suggests that location data should be considered highly sensitive.

13. As might have been foreseen, in order to share information rapidly to deal with the emergency created by the Covid-19 pandemic, privacy safeguards in NSW have been circumvented. Government agencies have not needed to seek exemption from privacy restrictions, instead relying on the provisions of the *Public Health Act 2010* and Orders.[9]

    Certainly, leveraging technological and other emergency options during a crisis, should not mean sacrificing personal privacy. "Even if there is some necessity for privacy intrusions for public health purposes (e.g., through such interventions as contact tracing), these invasions might not lead to the worst harms if they are conducted carefully and according to a set of transparent and consistent standards."[10]

14. A level of trust in the NSW government, has been the key factor in the early success of the government response to COVID-19. The Act should be drafted in such a way that it minimises the social implications of privacy violations in order to maintain the public's trust and governmental accountability.

---

[9] *New South Wales Public Health (COVID-19 Restrictions on Gathering and Movement) Order 2021*

S42 Direction of Minister concerning information exchange

(1) The Minister directs that a government sector agency or a NSW Minister (the first agency) is authorised to collect information from, or use or disclose information to, a related agency if the first agency considers it necessary to do so for the purposes of protecting the health or welfare of members of the public during the COVID-19 pandemic.

Information includes personal and health information.

[10] Boudreaux, B, Denardo, M.A., Denton, S.W., Sanchez, R., Feistel, K., Dayalani, H. 2020) Data Privacy During Pandemics A Scorecard Approach for Evaluating the Privacy Implications of COVID-19 Mobile Phone Surveillance Programs *RAND Corporation* p.31

15. The NSW government wants its citizens to maintain their willingness to comply with Public Health Orders and feel confident in getting tested. The Act should address more fully the necessary safeguards to ensure that information is not misused, misinterpreted and represented in a way that creates stigma or vilifies groups in our society.

    A case, in point, is the proposed collection of data on ethnicity for virus tests and vaccinations.[11] While the public health benefits are important, the Act, in its present incarnation, does not afford the necessary protections from unnecessary use and misuse of sharing data.

**Government Sector Agencies**

16. Government sector agencies are authorised to share data with another government sector agency for specific purposes under the Act.[12] Government sector agencies include not just the DAC and the various statutory bodies of the government but also local councils, State owned corporations and other bodies created by statute.

17. Data is shared with agencies operating under different statutes with their own rules on data use and disclosure. S6(2) of the Act requires that the data provider and recipient comply with the data sharing safeguards applicable to them. NSWCCL considers that if data is shared between agencies, the Act needs to set higher standards for data sharing.

18. The purpose for which data is proposed to be shared and used should be assessed as appropriate having regard to its necessity, use, value to the public and whether there is a risk of loss, harm or other detriment to the community if the sharing and use of the data does not occur.[13] Any such assessment should be independent.

19. A proposed data recipient must be assessed as an appropriate public sector agency with whom data may be shared for a particular purpose having regard to whether they have the appropriate skills and experience and will restrict access to the data appropriately. This safeguard is built into the SA Act[14]

20. NSWCCL considers that data sharing of personal information should not occur between agencies if the limitation to specific purposes cannot be guaranteed. The results of the data-sharing must benefit the public overall, not business or management being prioritised above appropriate limitations of reuse.[15]

---

[11] Dalzell, S. (8 March 2021) Language, country of birth to be recorded during COVID vaccine and positive tests *ABC News* https://www.abc.net.au/news/2021-03-08/language-country-birth-recorded-covid-vaccine-positive-test/13219288

[12] Other legislation may contain specific provisions authorising or requiring the sharing of data by an agency with specified bodies or equivalent bodies in another jurisdiction.

[13] See the Trusted Access Principles in the *SA Public Sector (Data Sharing) Act 2016* https://www.dpc.sa.gov.au/responsibilities/data-sharing/information-sharing-in-south-australia/sharing-public-sector-data

[14] *SA Public Sector (Data Sharing) Act 2016* ibid

[15] Op.cit Andrews

21. Personal information containing personal data should generally stay with the authoritative source. NSWCCL agrees with the premise "that agencies which have legislative protections against inappropriate reuse of data, such as the ABS, are the most appropriate linkers and facilitators for broader access to unit record sensitive data."[16] The DAC has that role in NSW. In the absence of this condition there should be strict controls on who can access the data, with great oversight and monitoring of usage and threats.

22. Sharing more data will not necessarily lead to better outcomes and represents a technocratic approach to managing policy outcomes. "(W)hen it comes to sensitive data, especially unit record data with personal information, more sharing is simply not always the answer. It can create an unhealthy, costly and sometimes dangerous distraction from what could really drive better public outcomes."[17]

23. On 18 December 2020, the Auditor-General for New South Wales, Margaret Crawford, released a report criticising the effectiveness of Service NSW's handling of customers' personal information to ensure privacy. The damning report highlights the lack of understanding and commitment to proper privacy practices in the NSW public service.

    The report states that "Service NSW is not effectively handling personal customer and business information to ensure its privacy. It continues to use business processes that pose a risk to the privacy of personal information. … Previously identified risks and recommended solutions had not been implemented on a timely basis."[18]

    The Auditor-General made eight recommendations aimed at ensuring improved processes, technologies, and governance arrangements for how Service NSW handles customers' personal information. These included, as a matter of urgency, that Service NSW should, in consultation with relevant NSW government departments and agencies, and the Department of Customer Service, implement a solution for a secure method of transferring personal information between Service NSW and those agencies.

    There is therefore little reason to trust that Service NSW will protect personal sensitive information without supportive robust legislation.

**Privacy Safeguards**

24. The privacy safeguards in the Act are inadequate. Privacy safeguards benefit and protect government sector agencies from mistakes and embarrassment and should be embraced not treated as a hindrance to data sharing.

25. All the data provided to public sector agencies (whether personal or non-personal) was provided for a particular purpose. When individuals share their personal information

[16] Ibid Andrews
[17] Ibid Andrews
[18] See Auditor General's Report. https://www.audit.nsw.gov.au/our-work/reports/service-nsws-handling-of-personal-information

with government, it is generally because they have to. Government agencies typically collect our personal information because they can compel us by law, or because we want or need to access some kind of government service. This means that there are limited opportunities for citizens to opt-out of public sector data collection and use.

The default position should be that any disclosure of our personal information should only occur in very limited circumstances.[19]

26. The safeguards have been criticised as having "no detail as to technical, operational and legal data governance and data management."[20] At the least, detail like the SA *Public Sector (Data Sharing) Act 2016* should be included, as below:

> *Data retention and disposal must be assessed as appropriate having regard to the physical storage location of the data and linked data sets, whether the proposed data recipient has appropriate security and technical safeguards in place, the likelihood of deliberate or accidental disclosure or use occurring; and how the data will be disposed of.*[21]
>
> *The publication or other disclosure of the results of data analytics work conducted on data shared must be assessed as appropriate having regard to the nature of the proposed publication or disclosure; the likely audience of the publication or disclosure; the likelihood of identification of a person to whom the data relates.*
>
> *An assessment as to whether the results of the data analytics work or other data for publication or disclosure will be audited and whether that process involves the data provider.*

27. The Act provides that health and personal information can be collected only if it is in compliance with the privacy legislation.[22] The privacy legislation means the PPIP Act or the *Health Records and Information Privacy act 2002.* Ss 17 & 18 of the PPIP Act limit the use and disclosure of personal information.

28. S.17 of the PPIP Act permits the use of personal information for a purpose other than that for which it was collected if an individual has consented or the other purpose for which the information is used is directly related to the purpose for which the information was collected. [23]

S.18 of the PPIP Act provides that a public sector agency must not disclose personal information unless the disclosure is directly related to the purpose for which the information was collected, it is not believed that the individual concerned would object to the disclosure.

---

[19] Op.cit Floreani

[20] Leonard, P (2020) Data Use and Data Sharing in Government New Regulations, Models and Challenges *Data Synergies* https://www.infogovanz.com/wp-content/uploads/2020/03/Peter-Leonard-Data-Use-and-Data-Sharing-in-Government-New-Regulations-Models-and-Challenges-9-March-2020.pdf

[21] Op.cit. *SA Public Sector (Data Sharing) Act 2016*

[22] S 12 Act

[23] Or if there is a serious or imminent threat to life or health of the individual. s. 17(c) and 18(1)(c) PPIP Act

If personal information is disclosed, as provided, the recipient agency must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

29. There are a number of exemptions to ss 17 and 18 and other sections of the PPIP Act. These relate to law enforcement, ASIO, investigative agencies, ICAC or public sector agencies lawfully authorised not to comply, as well as others.

30. Should one be harmed, as a result of the disclosure of personal information, a complaint will have little effect if disclosure is authorised by the PPIP Act. NSWCCL calls for a review of the PPIP Act to meet community expectations of privacy and, amongst other things, remove excessive exemptions and prevent overriding of the PPIP Act by other statutes.

**Recommendation 1**

NSWCCL considers that it is a misuse of information to use it for a purpose other than that for which it was obtained. All information whether personal or not should not be shared unless consent for that secondary or repurposed use has been obtained. Personal information should not be shared if the limitation for specific purpose cannot be guaranteed.

**Recommendation 2**

The Act should encompass provisions for independent assessment of the appropriateness of the purpose for which data is proposed to be shared and used. The assessment should have regard to its necessity, use, value to the public and whether there is a risk of loss, harm or other detriment to the community if the sharing and use of the data does not occur.

**Recommendation 3**

An assessment regime should be included in the Act to ascertain the appropriateness of:

a) the information to be shared, including whether it is appropriate to be shared at all, or stay with the authoritative source,
b) the agency to receive the information, having regard to the whether the agency has the appropriate skills and experience and will restrict data appropriately.

**Recommendation 4**

Personal information should be shared only in exceptional circumstances, in a safe and controlled manner and provided that it can be established that privacy interests should be outweighed.

**Recommendation 5**

If personal information is shared that information needs to be anonymised or deidentified according to a strict protocol which includes an assessment as to whether data may be reidentified.

**Recommendation 6**

The Act is inadequate in terms of its privacy safeguards. The Act should include necessary technical, operational and legal data governance and data management provisions.

**Recommendation 7**

To minimise the social implications of privacy violations and maintain accountability there should be auditing and reporting provisions in the Act. Those provisions should address, at the least, details of:

a) the nature of data being collected,
b) data destruction in accordance with agreed time limits,
c) compliance with consent provisions,
d) details of any complaints.

**Recommendation 8**

NSWCCL considers that there should be developed and included in the Act a set of transparent and consistent standards so that privacy is not circumvented during an emergency.

**Recommendation 9**

The definition of Government Sector Data is too broad and limitations on the type of data to be shared should be set out in the Act.

**Recommendation 10**

The number and type of agencies included in the definition of government Sector agencies is too broad. Data recipients should be assessed independently as to their appropriateness to receive the data.

**Recommendation 11**

NSWCCL considers that the Act relies too heavily on the PPIP Act which may be overridden by other statutes and has too many exemptions in its operation. NSWCCL strongly recommends a review of the PPIP Act.

This submission was prepared by Michelle Falstein on behalf of the New South Wales Council for Civil Liberties.

Yours sincerely,

**Michelle Falstein**
**Secretary**
**NSW Council for Civil Liberties**

Contact in relation to this submission- Michelle Falstein:
email michelle.falstein@nswccl.org.au;
tel 0412980540