Australian Government
Office of the Australian Information Commissioner

www.oaic.gov.au
GPO Box 5218 Sydney NSW 2001
P +61 2 9284 9800 F +61 2 9284 9666
E enquiries@oaic.gov.au
Enquiries 1300 363 992 TTY 1800 620 241
ABN 85 249 230 937

Our reference: D2017/001841

Senator Rachel Siewert
Chair, Senate Community Affairs References Committee
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Senator

Submission to Inquiry into the Better Management of the Social Welfare System initiative

I welcome the opportunity to comment on the Inquiry into the Better Management of the Social Welfare System initiative.

As the Committee may be aware, my Office, the Office of the Australian Information Commissioner (OAIC), has been in contact with the Department of Human Services (DHS) following the recent media coverage of Centrelink's automated data-matching and debt recovery system.[1] A number of matters that have been reported in the media appear to have privacy implications, including whether DHS has taken reasonable steps to ensure the accuracy of personal information used in the data-matching and debt recovery process, and whether individuals have had a reasonable opportunity to access and correct that personal information.

My Office has also been in regular contact with the Commonwealth Ombudsman's Office regarding its current own motion investigation into the matter. As the Commonwealth Ombudsman's investigation is ongoing, I have decided not to take any action at this point in time. I intend to review my position when the Ombudsman's report is available, after I have considered the Ombudsman's findings and recommendations.

In this submission, I have set out some relevant matters for the Committee's consideration. By way of a general comment, I acknowledge the importance of data-matching initiatives which aim to ensure people are receiving the correct amount of government assistance, and note that I am broadly supportive of such activities where they are used as a means of upholding the integrity of the Australian welfare system. However, I also note that where the data used in such activities is derived from personal information entrusted to the

[1] See the OAIC's media release on the OAIC website: Centrelink debt recovery system, 6 January 2017: https://www.oaic.gov.au/media-and-speeches/statements/centrelink-debt-recovery-system

government, it must be respected, protected and handled in a way that is commensurate with broader community expectations.

This is particularly important in circumstances where government agencies have the legal authority to collect, use and disclose personal information on a compulsory basis, or in exchange for access to essential government payments or services. Even where an agency may have this legal authority, consideration must be given to whether their use of personal information strikes an appropriate balance between achieving policy goals, and any impact on privacy. As part of this, agencies need to assess whether their handling of personal information is consistent with the community's expectations, and ensure that they have a social licence for any new uses of data.

The OAIC's supervisory role in relation to data-matching activities

The OAIC is an independent Commonwealth statutory agency. The OAIC was established by the Australian Parliament to bring together three functions:

- privacy functions (protecting the privacy of individuals under the *Privacy Act 1988* (Privacy Act), and other Acts)
- freedom of information functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (FOI Act), and
- information management functions (as set out in the *Information Commissioner Act 2010.*

In addition, the OAIC has regulatory oversight of government data-matching activities. Agencies that carry out data-matching must comply with the Privacy Act and other relevant legislation. For example, government data-matching between agencies such as the Australian Taxation Office (ATO), the Department of Veterans' Affairs (DVA) and DHS that involves the use of Tax File Numbers (TFN) is subject to the requirements of the *Data-Matching Program (Assistance and Tax) Act 1990* (Data-matching Act) and the *Guidelines for the Conduct of Data-Matching Program* (statutory data-matching guidelines).[2] The statutory data-matching guidelines are a legislative instrument, and the OAIC oversees compliance with these.

Agencies can also conduct data-matching for a range of other purposes, such as data-matching that involves the matching of data obtained from other Australian government agencies, state government agencies or private sector organisations. For these general types of data-matching which do not use TFNs, the OAIC has issued the *Guidelines on Data-matching in Australian Government Administration* (voluntary data-matching guidelines).[3] These guidelines are issued under s 28(1)(a) of the Privacy Act, and while not legally-binding, they represent the OAIC's view on best practice with respect to agencies undertaking data-matching activities. The voluntary data-matching guidelines therefore aim to assist agencies

[2] A link to the statutory data-matching guidelines is available on the OAIC's website: https://www.oaic.gov.au/agencies-and-organisations/legally-binding-guidelines-and-rules/legislative-datamatching-program-annotated-september-1991.

[3] A link to the voluntary data-matching guidelines is available on the OAIC's website: https://www.oaic.gov.au/agencies-and-organisations/advisory-guidelines/data-matching-guidelines-2014.

to use data-matching as an administrative tool, in a way that not only complies with the Australian Privacy Principles (APPs), but is also consistent with good privacy practice.

The obligations of DHS when data-matching

I understand that prior to the introduction of the new data-matching program, DHS and the ATO conducted their data-matching activities using TFNs under the Data-matching Act and the associated statutory data-matching guidelines. However, DHS's new data-matching program does not require the use of TFNs and DHS has therefore applied the voluntary data-matching guidelines. When compared with the requirements of the Data-matching Act, the voluntary data-matching guidelines provide more flexibility as to how data-matching activities may be conducted. Further, they do not place any restrictions on the volume of data matching that can be conducted. However, the guidelines do set out specific requirements and guidance to assist agencies comply with the APPs.

The voluntary data-matching guidelines require agencies to develop a data-matching program protocol to inform the public of the existence and nature of the program. Protocols must contain the information set out in the guidelines, this includes a description of the data to be provided and the methods to be used which will ensure the data is of sufficient quality and accuracy for use in the data-matching program.[4] This reflects the principles contained in APP 10, which requires agencies to take reasonable steps to ensure that the information it uses or discloses, having regard to the purpose of the use or disclosure, is accurate, up-to-date, complete and relevant. A copy of the program should be provided to the OAIC and generally made publicly available.[5]

Under voluntary data-matching guidelines agencies also have a responsibility to notify the public of a data-matching program.[6] This reflects the principles of APP 5, which requires entities to notify the individual of the collection of their personal information. There are also specific requirements under the guidelines to notify individuals of proposed administrative action, and to give the individual the opportunity to respond.[7]

Quality of personal information – APP 10

As outlined above, some media commentary has suggested that there may be issues with the quality and accuracy of the information being used to assess Centrelink debts. For example, the following matters have been highlighted:

- the practice of annualising of income. This relates to DHS obtaining income data from the ATO and averaging it out over the financial year, instead of applying the income to the

[4] See Guideline 3 of the voluntary data-matching guidelines, available on the OAIC's website.

[5] Where the head of an agency considers that it would be appropriate, having regard to the public interest, to conduct a data matching program that would be inconsistent with one or more of the Guidelines, they can apply to the Commissioner for an exemption. For more information, see Guideline 10 of the voluntary data-matching guidelines, available on the OAIC's website.

[6] See Guideline 5 of the voluntary data-matching guidelines, available on the OAIC's website.

[7] See Guideline 6 of the voluntary data-matching guidelines, available on the OAIC's website.

fortnightly period in which it was actually earnt. It has been reported that this practice may give an inaccurate estimate of a recipient's income, leading to incorrect decisions

- the use of automated data-matching processes, resulting in the duplication of income in instances where the employer name on the ATO's records differs to the name reported to Centrelink by the individual. In such cases, it has been reported that the relevant algorithm fails to identify that the two employers are in fact the same, and applies the income to the individual's record again, resulting in an incorrect debt amount
- some individuals claim not to have received notification of a debt until they are contacted by a debt collector. This issue appears to relate to historical debts, where an individual may not have been a Centrelink customer for some time and their debt assessment and notification letters are therefore sent to an out-of-date address.[8]

DHS appears to have used a number of these practices for some time.[9] However, DHS has substantially increased the volume of data-matching being conducted as part of the new data-matching program and has automated some of these processes. DHS now also places the onus on the individual to establish whether any of the ATO data used is not accurate (whereas previously, DHS appears to have taken additional steps to contact the employer to seek the information or evidence needed, if the customer was unable to supply information). Regardless of whether these processes have been utilised previously, DHS has a continuing obligation to ensure that its data-matching program complies with the requirements of APP 10, to take reasonable steps to ensure the information it uses is accurate, up-to-date, complete and relevant.

The APP Guidelines provide various examples of what may constitute 'reasonable steps' to ensure the accuracy and quality of personal information, including:

- providing individuals with a simple means to review and update their personal information on an on-going basis, for example through an online portal
- reminding individuals to update their personal information each time the entity engages with the individual
- contacting the individual to verify the quality of personal information when it is used or disclosed, particularly if there has been a lengthy period since collection, and
- if the personal information is to be used or disclosed for a new purpose that is not the primary purpose of collection, assessing the quality of personal information, having regard to that new purpose before the use or disclosure occurs.[10]

As outlined above, I intend to review the Commonwealth Ombudsman's report when it becomes available, to assess the above matters and determine whether any action is required

---

[8] I understand from the information provided by DHS during the Senate Committee's public hearing of 8 March 2017 that DHS is now sending all letters via registered mail to ensure they are received. Where letters are returned, DHS is then taking additional steps to contact the individual or obtain a current address from publicly available sources, such as the electoral role.

[9] Based on the information provided by DHS during the public hearing of 8 March 2017

[10] See Chapter 10: APP 10 – Quality of personal information of the APP Guidelines, available on the OAIC's website

by my Office. In the meantime, I would encourage DHS to ensure it takes reasonable steps to ensure that its data-matching activities comply with its obligations under APP 10, in light of the issues raised above.

Correction of personal information

APP 13 requires an entity to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading. This requirement applies where:

- the entity is satisfied the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, or
- the individual requests the entity to correct the personal information.

I understand from media reports that some individuals may have experienced difficulties when attempting to change or correct the matched data that is presented to them in the online compliance intervention platform. Some individuals have also alleged that they are facing difficulties when attempting to upload evidence and documents to the platform.

While APP 13 does not stipulate formal requirements that an individual must follow to make a request for correction of their personal information, an entity must state in its APP Privacy Policy how an individual may make a correction request.[11] While entities are permitted to draw individuals' attention to their preferred channels for making correction requests, they cannot require an individual to follow a particular procedure. Any recommended procedures should be regularly reviewed to ensure that they are flexible, and that they facilitate rather than hinder the ability of individuals to correct their personal information.[12]

I note DHS has advised that it has reviewed the online compliance intervention platform, to allow individuals more flexibility to provide net income figures and bank statements as evidence.[13] I encourage DHS to conduct regular reviews in order to ensure that the methods it is providing to individuals to enable corrections are flexible and facilitative. This is also a matter that I intend to reassess once the Commonwealth Ombudsman's report is available for review.

Community expectations

The community's response to this issue has demonstrated that Australians are increasingly aware of privacy issues, especially in light of new technological advances. People expect government agencies to act transparently when handling their personal information, and these expectations are heightened when information has been collected on a compulsory basis, or in exchange for access to essential payments and services.

---

[11] See APP 1.4(d).

[12] See the APP Guidelines, Chapter 13, available on the OAIC's website for more information

[13] Based on the information provided by DHS during the public hearing of 8 March 2017

The media reports on this matter have demonstrated how privacy concerns can escalate quickly and have the potential to impact on community trust. This is of particular relevance given the Australian Government's broader data innovation agenda and the move to a 'digital first' service delivery model across the Australian Public Service (APS).

It is therefore particularly important that agencies involved in data-matching or other new information-handling practices are as transparent as possible about their data practices. Good privacy practice, together with effective communication and community engagement strategies, can help to ensure that the handling of personal information is consistent with the community's expectations. In turn, having a social licence for any new uses of data will help ensure the success of projects that rely on the use of personal information.

If you wish to discuss any of these matters further, please contact Sarah Ghali

Yours sincerely

Timothy Pilgrim PSM
Australian Information Commissioner
Australian Privacy Commissioner

22 March 2017