



**Australian
Privacy
Foundation**

<http://www.privacy.org.au>

Secretary@privacy.org.au

<http://www.privacy.org.au/about/contacts>

15 November 2022

Ms Natalie Connell
Acting National Manager
myGov Customer Experience and Engagement
Digital Programmes Division
Department of Human Services

Dear Ms Connell

**Re: Response to Services Australia request for comments on
“myGov Increased Capture of Customer Data Feedback and Consultation”**

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached.

Thank you for the opportunity to contribute to the thinking about collecting customer data in the operation of myGov. The APF is always ready to assist with feedback on such proposals.

We are generally blunt and direct in responding to requests for comment and aim to “cut to the chase” and offer observations as we see them, though we do appreciate that there are always many other factors which may need to be considered.

We understand the focus of this exercise is to explore the basis of user trust in extending the functions of myGov. **Our concern is in understanding what the system is proposed to achieve and how it works in order to assess the value/risk compromise made by citizens who are obliged to use myGov and the associated agency systems.**

Unfortunately, we have had difficulty understanding many of the aspects of your intended initiative. Much of the information in your document is vague, ill-defined and generally uninformative regarding the goal you are attempting to achieve and the approach you are adopting.

In your first paragraph of “Context & myGov Vision” starts with

“At it’s core, the role of myGov as described by Minister Shorten, is to establish a ‘single front door’ for government services and support the delivery of these services for customers.”

Nowhere do you define what you are attempting to achieve with a goal of “single front door”. This could be anything from a simple single-sign on (much as at present) to a tight integration of multiple existing government agency systems, each with their own data definitions and rules for their use. The functionality, value and consequential risks vary with both the goal and implementation.

The current myGov is the only way citizens can access some agencies. Do you intend to maintain this restriction and increase the number of agencies subject to it? Do you intend to make myGov the only means by which citizens can engage most if not all government agencies?

There is reference to myGov capturing new data, for which you appear to be requesting advice and consent. For myGov to work with existing systems, requires access to at least some data in these systems. What is the intention regarding these data flows? Do you intend integrating existing agency systems via myGov to facilitate data matching across multiple agencies? (see Figure 2: Definitions of how data can be handled in myGov – Use, Collect and Match segments) Your document is ambiguous regarding what you are really trying to achieve; in fact, the document raises more questions than it answers.

Unless we know at a reasonable level of detail what the new myGov is supposed to be doing and its long-term development, it is impossible to comment on how you propose to do it and if it is acceptable from a data privacy perspective.

The issue of privacy, like any other aspect of an IT system should not and cannot be treated in isolation. In order to assess the privacy requirements, risks and mediation initiatives, means having knowledge of the whole system and an indication of how it will, or is supposed to, work.

When defining a large-scale Information System, it is usual to have a detailed description of the problem that requires addressing and a high-level description of the proposed system identifying the major components and their interactions. This is known as a system architecture. There are two possibilities:

- You have a system architecture which you are not sharing with us and which is predicated on decisions already made; and
- You do not have a systems architecture.

In the first case, you will already have made decisions regarding the system and this exercise in consultation is simplistic and designed to imply consent from various stakeholders.

In the second case, there are two possibilities. It could mean you understand the problem but have not formalised it in an architecture document, or you have not analysed the problem. Whatever the situation, it is unclear if you understand the many issues that need addressing when integrating multiple, disparate, existing systems, not the least of which is data consistency – or lack of, which was the problem with RoboDebt.

This issue is key in developing trust – it is difficult to for us and people generally to have confidence you have adequately identified and mitigated the risks of holding citizens' data.

Australians are a disparate group of citizens with many different age-groups, needs, capabilities, cultures and concerns. You run the risk of treating them all as one monolithic group with one and only one mechanism by which they can interact with the Government.

The Government has been advised many times over many years to have multiple channels through which citizens can interact with agencies. It might suit some people to have a single point of contact using digital tools, others may prefer to interact directly with each agency using some other method.

The proposed myGov vision seems to be a government-created funnel down which all citizens will be forced. It is the IT equivalent of kettling, a term coined to describe the actions by the London police in controlling crowd behaviour whereby there is one and only one way for people to proceed. Personalisation is too little too late.

It is possible that we may have misunderstood what you are trying to achieve, but the information you have provided is lacking in the detail and substance that would allow us to come to a rational, clear and unambiguous conclusion.

If you provide us with a more comprehensive description of the problem you are attempting to solve and proposed solutions, we would be in a better position to offer informed observations on the privacy aspects of the system, and how they might be perceived by Australians trying to understand whether the result would be sufficiently trustworthy to use.

If you feel it would be useful, we would be happy to engage in a less formal conversation regarding the issues we have raised. Please contact myself and Dr Bernard Robertson-Dunn.

Thank you for your consideration.

Yours sincerely



David Vaile, Chair, in conjunction with Dr Bernard Robertson-Dunn
For the Board of the Australian Privacy Foundation

0414 731 249
0411 157 113

David.Vaile@privacy.org.au
Bernard.Robertson-Dunn@privacy.org.au

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, Committees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby and Elizabeth Evatt, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policy Statements <https://privacy.org.au/policies/>
- Policy Submissions <https://privacy.org.au/publications/by-date/>
- Media Releases <https://privacy.org.au/media-release-archive/>
- Current Board Members <https://privacy.org.au/about/contacts/>
- Patrons and Advisory Panel <https://privacy.org.au/about/contacts/advisorypanel/>

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) <https://privacy.org.au/about/history/formation/>
- Credit Reporting (1988-90) <https://privacy.org.au/campaigns/consumer-credit-reporting/>
- The Access Card (2006-07) <https://privacy.org.au/campaigns/id-cards/hsac/>
- The Media (2007-) <https://privacy.org.au/campaigns/privacy-media/>
- My Health Record (2010-20) <https://privacy.org.au/campaigns/myhr/>