ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA

ART 2025/4916

BETWEEN

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

APPLICANT'S STATEMENT OF ISSUES, FACTS AND CONTENTIONS

1. The applicant seeks review of a decision by the respondent to refuse the applicant's request to access the source code of the Android version of the myGov Code Generator app (**App source code**) under the *Freedom of Information Act 1982* (Cth) (**FOI Act**). The applicant's freedom of information (**FOI**) application was refused pursuant to s 47E(d) of the FOI Act. In this review before the Administrative Review Tribunal (**Tribunal**), the respondent argues that the Code Generator app source code is exempt from disclosure under ss 33(a)(i) and 47E(d).

2. The proceeding is to be heard in the Intelligence and Security Jurisdictional Area (**ISJA**) of the Tribunal.

PART I ISSUES

3. The issues for determination by the Tribunal are whether the App source code is exempt from disclosure under:

   3.1. s 33(a)(i) of the FOI Act on the ground that disclosure would, or could reasonably be expected to, cause damage to the security of the Commonwealth; and/or

   3.2. s 47E(d) of the FOI Act on the ground that disclosure would, or could reasonably be expected to, have a substantial adverse effect on the proper and efficient conduct of the operations of an agency and that disclosure at the time of the Tribunal's decision would, on balance, be contrary to the public interest.

4. The onus is on the respondent to establish that at least one of the exemptions applies.

PART II FACTS

FOI request

5. On 13 July 2021, the applicant made a request to Services Australia under the FOI Act for access to (**T5**):

   > (1). Source code of the myGov Code Generator iOS and Android apps, including build scripts, manifests, software license terms, and media assets (icons, audio files, etc).

Lodged on behalf of the Applicant
Applicant contact: Jason Bosland

Wise Law
141A Como Parade East
Parkdale Vic 3195

Telephone: 0421 193 711

Email: JB@wiselaw.com.au

(2). Technical documentation describing the operation of the myGov Code Generator app, such as design documents, architecture diagrams, API documentation, security assessments, technical presentation slides, and similar documents.

If it assists in the expeditious processing of my request, source code may be delivered as a "snapshot" or export source repositories, in ZIP, "tarball" or similar format. However, the full development history is preferred.

6. On 13 September 2021, the respondent refused the applicant access to 12 documents falling within the scope of the request on the basis that disclosure would or could reasonably be expected to have a substantial adverse effect on the proper and efficient operations of the agency and that disclosure would be contrary to the public interest (the 'Primary Decision'). (**T2**)

Internal review

7. On 12 October 2021, the applicant sought internal review of the Primary Decision. (**T6**)

8. On 11 November 2021, the respondent affirmed the primary decision on the basis that the requested documents were exempt under the FOI Act and, on balance, it would be contrary to the public interest to release this information. (**T3**)

Information Commissioner review

9. On 10 January 2022, the applicant sought review of the internal review decision by the Office of the Australian Information Commissioner (**'OAIC'**) (**T7**).

10. On 15 May 2023, Services Australia provided submissions to the Information Commissioner in support of the exemption claims (**T11**). Services Australia subsequently provided an affidavit of Mr Garrett McDonald dated 12 March 2025 to the Information Commissioner in support of the exemption claims (**T9**)**.**

11. On 6 June 2025, the OAIC issued a decision not to continue to undertake a review of the internal review decision under s 54W(b) of the FOI Act (**T4**)**.**

ART review application

12. On 4 July 2025, the applicant sought merits review from the Administrative Appeals Tribunal, consistently with s 57A(1)(b) of the FOI Act (**T1**).

13. On 23 January 2026, following an application from the respondent, Deputy-President Britten-Jones directed under s 134(2) of the ART Act that the Tribunal's powers in respect of this proceeding be exercised in the ISJA. Special rules set out in Part 6 of the ART Act apply when the Tribunal is exercising its powers in the ISJA. As the decision under review is not an intelligence and security decision (as defined in s 4 of the ART Act), the special rules in Part 6 that apply to this proceeding are limited to:

    13.1. section 145: Constitution of the Tribunal – general rule;

13.2. section 153: Tribunal may invite person to give evidence;

13.3. section 156: Duty of the Tribunal in relation to security and law enforcement information;

13.4. section 157: Restricting publication or disclosure of information; and

13.5. section 160: Protecting identities of persons giving evidence.

14. On 3 March 2026, following provision of joint proposed consent orders, Deputy President Dordevic made a decision under s 103(3) of the ART Act to limit the scope of the review to a single document, being the latest version of source code of the Android version of the App that was publicly available at the time of the applicant's original FOI request (13 July 2021).

PART III CONTENTIONS

15. The respondent contends that the App source code is an exempt document pursuant to s 33(a)(i) and s 47E(d).

16. The respondent relies upon the open and confidential affidavits of Mr Garrett McDonald (both affirmed on 25 May 2026) (**McD-OA** and **McD-CA**, respectively).

17. The applicant disputes the respondent's contention that the App source code is an exempt document under either s 33(a)(i) or s 47E(d). The applicant relies upon the expert reports of Professor Vanessa Teague (**Teague Report**) and Dr Peter Serwylo (**Serwylo Report**). The applicant also relies upon an affidavit by the applicant, affirmed on 29 July 2026 (**FT-A**).

18. Source code is the complete set of instructions for building and running an app, presented in human-readable form (**Teague Report [1]; FT-A [7]**). To the extent that the Tribunal finds the App source code to be an exempt document under either s 33(a)(i) or 47E(d), the applicant contends that the App source code can be disclosed with exempt material redacted or deleted in accordance with s 22(2) of the FOI Act.

Section 33(a)(i) – damage to security of the Commonwealth

19. Section 33(a)(i) provides:

> A document is an exempt document if disclosure of the document under this Act:
> (a) would, or could reasonably be expected to, cause damage to:
> (i) the security of the Commonwealth.

20. Section 33(a)(i) applies to exempt a document if disclosure of the document 'would or could reasonably be expected to…cause damage to the security of the Commonwealth.' The applicant agrees with the respondent that 'could' in this context is less stringent than 'would', and that it requires an analysis of reasonable expectation rather than certainty of an event, effect or damage. The applicant also agrees with the respondent that it does not require the Tribunal to be satisfied on the balance of probabilities (**RSOFIC [19]**). However, it is important to add that a reasonable expectation of damage to the security of the Commonwealth requires more than a mere possibility, risk or chance of that damage occurring as a result of disclosure.[1] Rather, there must be a real, significant or material possibility of such damage occurring,[2] based on 'real and substantial grounds.'[3] In other words, the Tribunal must be satisfied that the expectation of damage resulting from disclosure is 'reasonably based',[4] supported by sufficient evidence and cogent reasoning.

21. The causation requirement under s 33(a)(i) requires demonstrating that there are real and substantial grounds for expecting that the *disclosure* of the relevant document could reasonably be expected to *cause* the relevant damage. As stated by Davies J in *Re Maher and Attorney-General's Department,* '[t]here must be cause and effect which can reasonably be anticipated.'[5] That causal link may be difficult to establish, and may be impossible to establish entirely, where the information is already in the public domain and where the relevant damage could be caused by means unconnected to the disclosure. In relation to information that is already in the public domain, Deputy President Britten-Jones observed in *Patrick and Secretary, Department of Prime Minister and Cabinet (Freedom of Information)* that:

> I accept the contention from both parties that it is critical to consider the disclosure of the Disputed Material in the context of…information…that is publicly available. If the information in the Disputed Material is largely similar to the publicly available information then that will be an important factor in my consideration as to whether the Disputed Material would, or could reasonably be expected to, cause damage to the defence of the Commonwealth. It is axiomatic that if the Disputed Material discloses information that is already publicly available then it would not have, or could not reasonably be expected to have, the required causative effect. However, I accept the Secretary's submission that the Disputed Material must be seen

---

[1] *News Corporation Ltd v National Companies and Securities Commission* (1984) 5 FCR 88, 95, 101-2; *Re Maher and Attorney-General's Department* [1985] AATA 180 [41]; (1985) 7 ALD 731, 742.
[2] *Chemical Trustee Limited and Ors and Commissioner of Taxation and Chief Executive Officer, AUSTRAC (Joined Party)* [2013] AATA 623, [79].
[3] *Attorney-General's Department v Cockcroft* (1986) 10 FCR 180, 196 (Sheppard J).
[4] *Attorney-General's Department v Cockcroft* (1986) 10 FCR 180, 190 (Bowen CJ and Beaumont J).
[5] *Re Maher and Attorney-General's Department* [1985] AATA 180 [41]; (1985) 7 ALD 731, 742.

in its context and that the information in the Disputed Material is not all of the same character.[6]

Respondent's arguments and evidence

22. The respondent relies upon the affidavit evidence of Mr McDonald to make eight distinct arguments that disclosure of the App source code would, or could reasonably be expected to, cause damage to the security of the Commonwealth (**RSOFIC [32]-[37]**). The eight arguments are as follows:

    22.1. Access to the source code could be used by malicious actors to identify vulnerabilities within: (i) the App source code; (ii) the myGov Service; and (iii) possibly the Agency's systems more broadly (**McD-OA [39]**) (**vulnerability argument**).

    22.2. The App source code could be potentially analysed and used by malicious actors, including State actors, organised criminal syndicates and hackers, to identify possible weaknesses in the algorithm which make it easier to guess a TOTP and gain unauthorised access to a legitimate user's myGov account (**McD-OA [43.1]**) (**weaknesses in the algorithm argument**).

    22.3. The App source code, if disclosed, could be used by malicious actors, including State actors, organised criminal syndicates and hackers, to build a counterfeit app which legitimate myGov users might use to access their myGov account. The use of a counterfeit app by the legitimate myGov user could allow a malicious actor to obtain the victim's myGov user credentials and compromise their account. (**McD-OA [43.2]**) (**counterfeit app argument**).

    22.4. Disclosure of the App source code could, or may reasonably be expected to, provide a window into other source code used in the Agency's digital services, including, importantly, other parts of the myGov Service, such as source code for the main public-facing myGov System (**McD-OA [44.1]**) (**other source code argument**).

    22.5. Disclosure of the App source code could, or may reasonably be expected to, afford greater insight into the threat detection systems and tools the Agency uses and thereby permit malicious actors to use that information to devise ways to avoid detection (**McD-OA [44.2]**) (**avoid detection argument**).

    22.6. Disclosure of the App source code could, or may reasonably be expected to, facilitate the development or refinement of malicious tools or exploits to compromise myGov which could assist adversaries to bypass existing

[6] [2020] AATA 4964, [48].

myGov safeguards or cyber threat detection mechanisms. (**McD-OA [44.3]**) (**bypass safeguards/threat detections argument**).

22.7. Disclosure of the App source code may be significant to the application of 'mosaic analysis' which is the method by which an individual or entity can build up a coherent and comprehensive picture from individual pieces of information, including apparently innocuous or meaningless pieces of information (**RSOFIC [33]**; **McD-OA [45]-[47]**) (**mosaic analysis argument**). Mr McDonald deposes that '[t]he risk to the cybersecurity of a system due to this type of analysis in reinforced by ADS updating the ISM principles in March 2026 to introduce a principle entitled 'GOV-10-System exposure minimisation' (**GOV-10 principle**), which states:

> Information about the design, configuration and operation of systems (infrastructure, operating systems, applications and data) is not publicly disclosed or shared externally unless necessary for commercial, legal, regulatory or security purposes, with any disclosure minimised, controlled or logged.

22.8. Artificial Intelligence (**AI**) models could take advantage of the disclosure of the App source code to more easily and rapidly identify vulnerabilities in the code and develop working exploits for these vulnerabilities (**McD-OA [48]-[49]**) (**AI argument**).

23. It appears to the applicant that the respondent's case, in respect of each of the eight arguments, proceeds in three steps:

Step 1: the disclosure of the App source code would, or could reasonably be expected to, cause malicious actors, by engaging in activities identified in the respondent's eight arguments, to:

(a) exploit vulnerabilities in the myGov App, the myGov System more broadly and/or other Agency services; or

(b) obtain unauthorised access to the myGov Service and/or other Agency services.

Step 2: such exploitation or unauthorised access by malicious actors would, or could reasonably be expected to, result in certain undesirable consequences; and

Step 3: such consequences would, or could reasonably be expected to, cause damage to the security of the Commonwealth.

24. The applicant does not dispute Step 2 in the respondent's case with respect to each of the eight arguments. That is, the applicant does not dispute that the exploitation of vulnerabilities or unauthorised access by malicious actors as set

out in Step 1, if they were to materialise, would, or could reasonably be expected to, produce undesirable consequences.

25. Rather, the applicant's case is confined to rejecting Step 1 in the respondent's case in respect of each of the eight arguments – namely, that disclosure of the App source code would cause, or could reasonably be expected to cause, malicious actors to engage in any of the activities identified in the respondent's eight arguments. This is because the respondent has not established on the evidence the necessary causal link between disclosure of the App source code and a reasonable expectation that malicious actors would engage in the conduct identified in the respondent's case *as a result of the disclosure*. As the respondent's case for exemption is confined to the eight arguments identified in the respondent's submissions, the applicant contends that the respondent has not established that disclosure of the App source code would, or could reasonably be expected to, cause damage to the security of the Commonwealth.

26. The applicant addresses Step 1 in respect of each of the respondent's eight arguments in paragraphs [27]-[61].

Applicant's arguments and evidence

Vulnerability argument

27. The applicant rejects the respondent's argument that disclosure of the source code could be used by malicious actors to identify vulnerabilities within: (i) the App source code; (ii) the myGov Service; and (iii) possibly the Agency's systems more broadly (**McD-OA [39]**). Scopes (i), (ii), and (iii) are distinct and are dealt with separately below, in paragraphs [28]-[33].

<u>The App source code</u>

28. There are two bases upon which the applicant contends that disclosure of the App source code would not, and could not reasonably be expected to, cause malicious actors to identify vulnerabilities in the App.

29. First, disclosure of the App source code should not and normally would not disclose vulnerabilities in the App that cannot be discovered without access to the App source code (**Teague Report [48]**).

30. As outlined by Professor Teague (**Teague Report [58]**), access to the App's source code would reveal:

    30.1. details of the App's cryptography protocols;

    30.2. details of the App's dependencies, ie libraries used to implement the protocols;

30.3. details of the App's implementation choices – that is, extra details that are necessary for the cryptographic protocols to function, but are not specified in the standards that define the cryptographic protocols used by the App; and

30.4. details of communications between the App and the myGov servers (**API calls**).

31. The applicant contends that each of the details identified in paragraphs [30.1]-[30.4] can be ascertained without access to the App source code:

31.1. The App's cryptographic protocols, OAuth2.0 and TOTP, are public standards and are therefore already in the public domain (**Teague Report [13], [19], [27], [59]**).

31.2. Disclosure of the App's source code should not, and normally would not, reveal anything about the App's dependencies that cannot already be inferred from examining the App's compiled code (**Teague Report [59]**).

31.3. The implementation details of the App's functionality can be discovered by examining the App itself, including by decompilation (**Teague Report [59]**). Furthermore, such implementation details are already in the public domain (**Teague Report [59]**). Any implementation details that cannot be discovered by examining the App itself (for example, because they do not relate to the App's functionality), are highly unlikely to contain vulnerabilities in the App. Therefore, the disclosure of such implementation details could not be used by malicious actors to identify and/or exploit any vulnerabilities in the App.

31.4. The details of the App's API calls can be discovered by examining the App itself (**Teague Report [17], [59]-[61]**). Furthermore, most of the details of the App's API calls to the myGov server and the responses that it generates are already in the public domain (**Teague Report [61], [73]**).

32. Given that information in the App source code capable of revealing vulnerabilities in the App can be, and has been, ascertained without access to the App source code, disclosure of the App source code could not reasonably be expected to result in malicious actors identifying vulnerabilities in the App that could not otherwise be identified.

33. Second, the cryptographic protocols used by the App are highly unlikely to contain vulnerabilities. This is because both protocols are open, public standards and have been subjected to extensive scrutiny for vulnerabilities (**Teague Report [53], [66]-[70]**). Where vulnerabilities have been found, they have been corrected (**Teague Report [53]**). Given that the App's cryptographic protocols are highly unlikely to contain any vulnerabilities, it logically follows that disclosure of the App source code could not reasonably be expected to enable a malicious actor to identify any vulnerabilities.

The myGov Service

34. The applicant contends that disclosure of the App source code would not, and could not reasonably be expected to, disclose vulnerabilities in the myGov Service. The applicant takes the reference to the 'myGov Service' in Mr McDonald's affidavit (**McD-OA [39]**) to mean the Internet-exposed services with which the App interacts over the Internet, as well as the other Internet-exposed or 'back-end' services and systems which together comprise the whole myGov Service.

35. In relation to the myGov Internet-exposed services with which the App interacts, the only aspect of the myGov Service that disclosure of the App source code would be expected to reveal is the protocols used in the API calls, including what the API expects in, and how it responds to, an honest request from a client (**Teague Report [60]-[61], [73]**). The applicant contends that such protocols can already be ascertained by analysing the App itself, including through the decompilation of the App's compiled source code and the use of tools for observing what the App does while it is running (including observing what data the App is sending to or receiving from the myGov server) (**Teague Report [11]-[16], [61]-[62]**). Furthermore, the details of such protocols are already in the public domain (**Teague Report [61], [73]**). It follows that any vulnerabilities in the API protocols, if they exist, could be identified and exploited by malicious actors without access to the App source code. Disclosure of the App source code, therefore, could not reasonably be expected to reveal any vulnerability in the protocols used for communication between the App and the myGov server that are not already in the public domain or are not already discoverable by analysing the App itself.

36. In relation to myGov Internet-exposed services that the App does *not* interact with and other non-Internet exposed systems that make up the 'myGov Service', the App source code ordinarily would not, and should not, reveal such details (**Teague Report [45], [74]**). Of particular importance to the security of the myGov Service, disclosure of the App source code should not, and normally would not, reveal anything about any heuristic defences on the server side of the myGov Service, such as spam filtering or the ways that the server distinguishes between malicious fake logins from genuine forgotten passwords (**Teague Report [61], [74]**). Mr McDonald's open affidavit does not identify the means or mechanisms by which the App source code could reasonably be expected to reveal vulnerabilities in such non-Internet exposed systems or services. Furthermore, Mr McDonald's open affidavit does not point to the existence of any further evidence in his closed affidavit regarding such vulnerabilities.

37. The applicant concedes that the App source code may contain information about the overall myGov System which is both (a) not discoverable through analysis using the techniques described by Professor Teague (**Teague Report [11]-[16]**), and (b) which may be used by malicious actors to compromise the myGov system. For example, it is possible that the source code contains passwords (not

myGov user passwords), or secret keys used in cryptographic operations. Source code should not and ordinarily would not contain information of this character. However, to the extent that the App source code does in fact contain such information, the respondent has the burden of establishing what that information is and how it could reasonably be expected to be used by malicious actors to identify vulnerabilities in the myGov System. If the respondent is able to satisfy this burden, the applicant contends that such information can be redacted or deleted in accordance with s 22(2) of the FOI Act.

Other Agency services or systems

38. The App source code should not contain details about unrelated Agency systems. As Professor Teague states in her Report: 'I cannot think of any way in which the App's source code should, or normally would, reveal any vulnerabilities in services or systems it does not refer to or interact with' (**Teague Report [63]**).

39. Mr McDonald's affidavit does not identify the means or mechanisms by which the disclosure of the App source code could reasonably be expected to reveal vulnerabilities in unspecified Agency systems. Furthermore, Mr McDonald's open affidavit does not point to the existence of any further evidence in his closed affidavit regarding such vulnerabilities.

40. To the extent that the App source code does contain information about other Agency services or systems, the respondent has the burden of establishing what that information is and how it could reasonably be expected to be used by malicious actors to identify vulnerabilities in other Agency services or systems. If the respondent is able to satisfy this burden, the applicant contends that such information can be redacted or deleted in accordance with s 22(2) of the FOI Act.

Weaknesses in the algorithm argument

41. The algorithm of the App is the series of steps or instructions for generating TOTP codes from the current time and a shared secret (**the TOTP algorithm**) (**Teague Report [66]**). The applicant rejects the respondent's reliance upon Mr McDonald's evidence that disclosure of the App source code could potentially be analysed and used by malicious actors to identify possible weaknesses in the App's algorithm which make it easier to identify the TOTP and gain unauthorised access to a legitimate user's myGov account (**McD-OA [43.1]**). This is for three reasons:

    41.1. First, Mr McDonald states in his open affidavit that the App source code could *potentially* be used to reveal weaknesses in the algorithm but provides no further evidence as to *how* the App source code could be used in this way (**McD-OA [43]**). Furthermore, Mr McDonald's open affidavit does not point to the existence of any further evidence in his closed affidavit regarding how the App source code could reveal such weaknesses. A mere assertion of potentiality without explanation or evidence does not provide a sufficient basis to satisfy the Tribunal that

disclosure of the App source code could reasonably be expected to cause damage to the security of the Commonwealth.

41.2. Second, the applicant rejects that the App source code can be used in the way stated in Mr McDonald's affidavit. The TOTP algorithm used by the App is a public standard and all of its algorithmic details are already in the public domain (**Teague Report [67]**). The TOTP algorithm has been proven to be secure against malicious parties' attempts to guess an individual TOTP without knowledge of the shared secret (**Teague Report [67]**). It is therefore extremely unlikely that the TOTP algorithm has vulnerabilities that could be exploited by a malicious actor to guess a TOTP code significantly more effectively than random guessing (**Teague Report [68]**).

41.3. Third, even if the TOTP algorithm contains vulnerabilities, which the applicant does not accept, the TOTP algorithm is a public standard and therefore access to the source code is not required to discover such vulnerabilities, nor would it make such discoveries more likely (**Teague Report [69], [71]**).

Counterfeit app argument

42. The applicant rejects Mr McDonald's evidence that disclosure of the App source code would, or could reasonably be expected to, be used by malicious actors, including State actors, organised criminal syndicates and hackers, to build a counterfeit app which could then be used to obtain a victim's myGov user credentials and compromise their account (**McD-OA [43.2]**).

43. The applicant does not dispute that a malicious actor could use the App source code as a basis for the development of a malicious counterfeit app. However, the applicant contends that disclosure of the source code would not give rise to a reasonable expectation that malicious actors would, in fact, do so. This is for three reasons:

43.1. First, counterfeit applications that would enable malicious actors to steal victim's myGov credentials can be developed without access to the source code of the legitimate app (**Serwylo Report [6]; T11 [35]**). This can be done by copying the App's design elements.

43.2. Second, access to the App source code would not make building a counterfeit app any easier than simply using reference designs or screenshots of the original app (**Serwylo Report [8]**). Indeed, given the limited features of the myGov Code Generator App, access to the App source code would provide only limited assistance to a malicious actor in building a counterfeit app (**Serwylo Report [12]**).

43.3. Third, malicious actors would want to build counterfeit apps that behave differently from the legitimate app. It follows that a counterfeit app's

source code would necessarily be different from, and could not simply replicate, the App's source code. Access to the App source code would therefore not materially assist in building such an app (**Serwylo Report [10]**). Furthermore, the benefit of access to source code for malicious actors has been significantly diminished with the advent of generative AI, which can be used to create counterfeit apps without access to a legitimate app's source code (**Serwylo Report [15]**).

44. Further, even if the creation of counterfeit apps by malicious actors is assumed, whether based on the App's source code or not, there is no reasonable expectation that such counterfeit apps could be distributed to victims, or that victims could be induced to install and run the apps on their devices. This is for three reasons:

    44.1. First, counterfeit apps face significant barriers to distribution. The most likely distribution channel for counterfeit apps on Android devices is through the Google Play Store (**Serwylo Report [16]**). However, there are mechanisms in place that would prevent counterfeit apps being admitted to the Google Play Store. Counterfeit apps will be in breach of Google Play policies relating to 'impersonation' and 'intellectual property' rights (**Serwylo Report [22]**). An app developer is required to declare that the app does not violate either of these policies (**Serwylo Report [24]**). Once submitted, apps are then reviewed by Google for violations of the policies. If a violation is detected, the app is blocked from publication in the Google Play Store (**Serwylo Report [25]**). Google runs over 10,000 checks on every app submitted to Google Play (**Serwylo [28], Appendix 5, page 21).** In the unlikely event that a counterfeit app is published, once detected counterfeit apps can be reported and banned from the Google Play Store (**Serwylo Report [26]; [33]-[35]**).

    44.2. Counterfeit apps can also be downloaded and installed onto Android devices from unknown sources, such as websites or via email attachments. However, when this occurs, users are warned that they are installing an app from an 'Unknown Source' (**Serwylo Report [19]**). Moreover, Android users can only install an app downloaded from an unknown source when they 'opt-in' (**Serwylo Report [19], Annexure 10**). Therefore, given these protections, it cannot reasonably be expected that an Android user would be induced to install a counterfeit app downloaded from an unknown source.

    44.3. Second, Google Play also has processes in place to protect users against the installation of counterfeit apps. All Android devices come with a service called Google Play Protect pre-installed (**Serwylo Report [29], Annexure 21**). This service checks apps before they are installed to ensure that they are not malware or otherwise in violation of Google's 'Unwanted Software Policy' (**Serwylo Report [29], Annexure 18)**. The service also notifies Android users when an app installed on a user's device is discovered to be malware or in violation of the 'Unwanted

Software Policy' (**Serwylo Report [29]**). Furthermore, Android users with existing legitimate apps on their devices are protected from being tricked into replacing them with counterfeit apps through a mechanism called 'signature verification' (**Serwylo Report [31]-[32], Annexure 31, page 53**). Due to the 'signature verification' mechanism, an Android user with the legitimate myGov Code Generator app installed could only install a counterfeit version of an app if they manually uninstall the legitimate app or if they install a counterfeit version with a different identifier alongside the legitimate app (**Serwylo Report [32]**).

44.4. Third, assuming a user of the legitimate myGov Code Generator App is deceived into downloading and installing a counterfeit app, the counterfeit app could not be used to steal any details from the legitimate myGov Code Generator App or any other app on the user's device. This is because of the 'Application Sandbox', which isolates apps from each other (**Serwylo Report [36]-[38], Annexure 11**).

Other source code argument

45. The applicant rejects Mr McDonald's evidence in his open affidavit that access to the App's source code could, or may reasonably be expected to, provide a 'window' into other source code used in the Agency's digital services, including other parts of the myGov Service (**McD-OA [44.1]**). This is because details of the myGov System or other Agency Services that are not used or triggered by the App cannot be ascertained or inferred from examining the App's source code (**Teague Report [45]**). Furthermore, while details of the myGov System that *are* used or triggered by the App are revealed in the App source code, they are already ascertainable from an examination of the App as demonstrated by Professor Teague (**Teague Report [17]**) and are already in the public domain (**Teague Report [73]; FT-A [72]-[77], [84]**).

46. If Mr McDonald's evidence is relied upon to support the more abstract proposition that disclosure of the App source code could reasonably be expected to reveal the sort of source code favoured by Services Australia in delivering other myGov services or other digital services, it must be rejected as hypothetical and vague. Mr McDonald's affidavit identifies no factual basis upon which the Tribunal could conclude that such an expectation is reasonably based, nor does it explain how the App source code could be used in this way, or why this might be of concern. Furthermore, Mr McDonald's open affidavit does not point to the existence of any further evidence in his closed affidavit in this regard.

Avoid detection argument

47. The applicant rejects the respondent's reliance upon Mr McDonald's evidence that disclosure of the App source code could provide insight into threat detection systems and tools used by the Agency (**McD-OA [44.2])**. Such defences are not part of the App's cryptographic protocols and are not triggered by the intended use of the App by honest clients. Therefore, the App source code ordinarily would

not, and should not, reveal details about these defences (**Teague Report [45], [74]**).

48. The App source code may reveal that extra communications with the myGov server have been added to help the server distinguish the genuine myGov App from alternative implementations. However, if this is the case, such extra details can be identified without access to the App source code (**Teague Report [77]**).

49. The applicant concedes that it is possible that information about myGov threat detection systems and tools has been included in the documents comprising the App source code. For example, such information could be included as comments (non-functional descriptive text) within source code files, or could exist as, or within, separate documentation files. To the extent that the App source code includes any such information, it can be redacted or deleted in accordance with s 22(2) of the FOI Act.

Bypass safeguards/threat detections argument

50. The applicant rejects the respondent's reliance on Mr McDonald's evidence that disclosure of the source code could, or may be reasonably expected to, facilitate the development or refinement of tools or exploits to enable malicious actors to bypass existing safeguards or cyber threat detection mechanisms (**McD-OA [44.3]**). This is because the App source code should not reveal any details about existing myGov safeguards or cyber threat detection systems (**Teague Report [74]**). Therefore, disclosure of the App source code should not and normally would not disclose information that would help a malicious actor to develop or refine tools or exploits to bypass existing myGov safeguards or cyber threat detection systems (**Teague Report [78]**). To the extent that the App source code includes any such information, it can be redacted or deleted in accordance with s 22(2) of the FOI Act.

Mosaic analysis argument

51. The applicant contends that the Tribunal should reject the respondent's mosaic analysis argument, as well as Mr McDonald's evidence as to the mosaic analysis.

52. The applicant concedes that the 'mosaic analysis' is an accepted method used by courts and tribunals to evaluate the significance of documents, including in the national security and FOI contexts. However, the respondent does no more than merely assert that the consequences of disclosure of the App source code to the security of the Commonwealth may be assessed on the basis of mosaic analysis (**RSOFIC [24]**). The respondent does not point to any evidence, or provide any reasoning, as to how the application of the mosaic analysis would justify the Tribunal reaching the conclusion that disclosure of the App source code would, or could reasonably be expected to, damage the security of the Commonwealth.

53. In addition, Mr McDonald's open affidavit (**McD-OA [46]-[47]**) states that disclosure of the App source code 'may be significant to the application of the

"mosaic analysis"', but does not provide any specific details as to how the mosaic analysis might be applied in relation to the App source code or what other pieces of information might be relevant to the mosaic analysis of the App source code. His evidence does no more than raise mosaic analysis as a hypothetical possibility in the abstract. Furthermore, Mr McDonald's open affidavit does not refer to additional evidence in his closed affidavit in relation to the application of the mosaic analysis.

54. Mr McDonald deposes that the risk of mosaic analysis – that is, individuals putting together apparently innocuous pieces of information in order to produce a composite of information that can be put to nefarious uses – is 'reinforced' by the Australian Signals Directorate (**ASD**) updating the Information Security Manual in March 2026 to include the GOV-10 principle. However, contrary to Mr McDonald's assertion, there is no evidence that the GOV-10 principle was introduced due to concerns that malicious actors may use mosaic analysis to analyse otherwise innocuous or meaningless pieces of data or information, or that it was intended to prevent such analysis from occurring.

55. Reliance on the mosaic analysis requires more than mere assertion that it should be applied to support a conclusion in any given context. Rather, reliance upon the mosaic analysis requires the respondent to establish, on the basis of sufficient evidence and cogent reasoning, that the App source code, when combined with other identified information or categories of information, could reasonably be expected to cause damage to the security of the Commonwealth. By merely asserting the mosaic analysis without taking the argument or evidence any further, the respondent has failed to satisfy this burden.

56. Furthermore, acceptance of the mosaic analysis in the current matter without sufficient evidence and cogent reasoning as to how it should be applied in the particular circumstance of this case would undermine the purpose and operation of the FOI Act. This is because, if reliance upon mosaic analysis in the abstract, and by mere assertion, were accepted by the Tribunal in this case, it is difficult to conceive of a scenario in which the argument would not succeed. Indeed, acceptance of the mosaic analysis to find in favour of the respondent in the present circumstances would be tantamount to the Tribunal accepting that the mosaic analysis will always justify a finding that even the most innocuous or anodyne documents are exempt from disclosure under s 33(a)(i). Such an approach cannot be reconciled with the pro-disclosure objects of the FOI Act.

AI argument

57. The applicant concedes that Generative AI provides a powerful tool for identifying and exploiting security vulnerabilities in software (**Teague Report [91]**). However, for the following two reasons, the applicant contends that disclosure of the App source code could not reasonably be expected to cause malicious actors to engage in the activities identified in Mr McDonald's evidence (**McD-OA [48]-[49]**).

58. First, a malicious actor intent on identifying and exploiting vulnerabilities in the App can already use advanced AI models for such purposes, without access to the source code. A recent security incident involving OpenAI, a leading AI provider, led the company to make the following observation (**FT-A [66], FT-20; Teague Report [107]**):

> The incident also makes clear that advanced models can discover and exploit novel attack paths in real-world systems without source-code access. It highlights that advanced cyber capabilities must be developed alongside stronger safeguards and defensive tools.

59. The provision of the App source code is unlikely to confer any significant advantage to a malicious actor using advanced AI models to identify and exploit vulnerabilities in the App (**Teague Report [108]**).

60. Second, AI can be used not only by malicious actors, but also by cybersecurity defenders to identify and patch vulnerabilities. Indeed, the defensive use of AI has recently been endorsed by the Australian Cyber Security Centre (ACSC), a department of the ASD, in a document published jointly with the apex cyber security agencies of Canada, New Zealand, the UK and the USA entitled 'Five Eyes cyber security agencies statement – The AI shift in cyber risk: why leaders must act now' (**FT-A [63]-[64], FT-19, page 324-325**). It states (**FT-A, FT-19, page 325**):

> Adversaries are already using AI to move faster and more effectively. Defenders must do the same.
>
> Organizations that integrate AI tools into their security operations can detect vulnerabilities earlier, improve software quality, monitor unusual behaviour, and respond faster to incidents – reducing both the cost and impact of incidents.

As a responsible government agency dealing with sensitive data, it is expected that the respondent would follow the official advice of the ACSC and make proactive use of advanced AI models to identify and patch any vulnerabilities present in the source code of the *current version* of the myGov Code Generator App or present in the implementation of the myGov servers. If this is done, disclosure of the App source code could not reasonably be expected to cause malicious actors to engage in any of the activities identified in Mr McDonald's evidence.

Security by obscurity

61. The applicant further contends that the respondent's specific arguments set out above are each premised on the assumption that the disclosure of source code, on balance, inherently increases cyber security risks ('security by obscurity'). The applicant contends that such an approach is flawed for the following reasons:

61.1. Security by obscurity is at odds with accepted approaches to the security of software systems.

61.1.1. It is widely accepted that designs of cryptographic systems are likely to be more secure if they are subject to public review (known as 'Kerckhoffs' Principle) (**Teague Report [49]-[56]**).

61.1.2. The Australian Cyber Security Centre (ACSC), a department of the Australian Signals Directorate (ASD), has embraced 'radical transparency and accountability' over security by obscurity in developing guidelines for designing secure software (**FT-A [34]**).

61.1.3. The US National Institute of Standards and Technology has rejected security by obscurity and endorsed the principle that '[s]ystem security should not depend on the secrecy of the implementation or its components' (**Teague [89], Appendix I**).

61.1.4. Security by obscurity has also been rejected as a valid approach to software security by the UK's Government Digital Service and Central Digital Data Office (**FT-A [51]**).

61.2. Australian Government policy has embraced the position that source code developed for delivery of digital services should be publicly disclosed. The Digital Transformation Agency (DTA), an Australian Government agency, publishes the Digital Service Standard (**DSS**), which sets the requirements for the design and delivery of high-quality digital government services. Version 1.0 of the DSS (**DSS v 1.0**), which was in operation from 6 May 2016 until DSS v 2.0 replaced it on 1 July 2024, contained Criterion 8, which required agencies to 'Make all new source code open by default' (**FT-A [19]-[21], FT-2, page 27**). Criterion 8 reflected the recognition that 'security by obscurity' does not guard against cyber security threats (**FT-A [22]-[24])**. Criterion 8 was omitted from DSS v 2.0; however, this was not for security reasons (**FT-A [27]-[33]**). A well-known example of an agency following Criterion 8 is the disclosure of the source code of the COVIDSafe contact tracing app, which has many similarities to the myGov Code Generator App (**FT-A [36]-[42]).**

61.3. Many other comparable jurisdictions have adopted open source policies for the delivery of services by government agencies, including the USA, UK, Finland and New Zealand, as well as five Australian state governments (**FT-A [45]-[54]**).

61.4. Some jurisdictions have legislated that software developed by government services must be open source. A recent example is the requirement in the EU that the 'source code of the application software components of European Digital Identity Wallets must be open-source licensed' (**FT-A, [60], FT-18, page 285**).

Application of s 47E(d) – effect on the proper and efficient conduct of an Agency

62. Section 47E(d) of the FOI Act provides:

> A document is conditionally exempt if its disclosure under this Act would, or could reasonably be expected to, do any of the following:
>
> …
>
> (d) have a substantial adverse effect on the proper and efficient conduct of the operations of an agency.

63. Section 11A(5) of the FOI Act provides:

> The agency or Minister must give the person access to the document if it is conditionally exempt at a particular time unless (in the circumstances) access to the document at that time would, on balance, be contrary to the public interest.

64. Section 11B(3) of the FOI Act articulates a non-exhaustive list of public interest factors favouring access where disclosure would:

> (a) promote the objects of this Act (including all the matters set out in ss 3 and 3A);
>
> (b) inform debate on a matter of public importance;
>
> (c) promote effective oversight of public expenditure;
>
> (d) allow a person to access his or her own personal information.

65. Section 11B(5) of the FOI Act requires the decision maker to have regard to the Guidelines:

> In working out whether access to the document would, on balance, be contrary to the public interest, an agency or Minister must have regard to any guidelines issued by the Information Commissioner for the purposes of this subsection under section 93A.

66. Pursuant to s 93A of the FOI Act, the Information Commissioner has issued guidelines (**Guidelines**) in relation to the public interest exemption. The latest version of the Guidelines (compiled July 2026) is available at: https://www.oaic.gov.au/freedom-of-information/freedom-of-information-guidance-for-government-agencies/foi-guidelines.

67. The Guidelines clarify that the four factors set out in s 11B(3) of the FOI Act must be considered if relevant (**Guidelines [6.229]**). The Guidelines also clarify that the four factors favouring disclosure in the FOI Act are non-exhaustive, and set out an extended non-exhaustive list of factors (**Guidelines [6.231]**). The extended factors, as relevant to the present matter, include:

> (b) inform debate on a matter of public importance…;

…

(c) promote effective oversight of public expenditure;

…

(i) advance the fair treatment of individuals and other entities in accordance with the law in their dealings with agencies;

…

(k) contribute to innovation and the facilitation of research.

68. The applicant does not take issue with the respondent's statements of general principle relating to the application of s 47E(d) (**RSOFIC [42]**).

Respondent's arguments and evidence

69. The respondent contends that the conditional exemption under s 47E(d) is satisfied because disclosure of the App source code could reasonably be expected to have a substantial adverse effect on the proper and efficient administration of the myGov Service, and related digital services and infrastructure. In particular, the respondent contends that the reasonably expected cyber security risk that he claims would result from the disclosure of the App source code would require the Agency to significantly increase resourcing and require the redeployment of existing resources to protect the myGov System and other Agency services (**RSOFIC [43])**. The respondent relies upon Mr McDonald's evidence that disclosure of the App source code would require 'significant additional funding and resourcing to be allocated to maintaining and protecting the security of myGov' to what he anticipates will be a 'significant increase in cyber security attacks' (**McD-OA [56]**).

70. The respondent also contends that access would, on balance, be contrary to the public interest under s 11A(5). This is based on the respondent's contention that the Government's ability to maintain the security of its systems significantly outweighs public interest considerations in favour of disclosure, including the public disclosure of the Government's approach to handling of technical protocols to secure its systems (**RSOFIC [45]**).

Applicant's arguments and evidence

Application of s 47E(d) - conditional exemption

71. The respondent's arguments and evidence claim that a 'significant increase' in cyber attacks is 'reasonably expected' and 'anticipated' as a result of release of the App source code, but do not provide any evidence in support of these claims, nor explain how that expectation is reasonable (**RSOFIC [43]; McD-OA [56]-[57]**). The applicant infers, and contends that the Tribunal should also infer, that the respondent seeks to establish this by the same evidence and contentions relied upon to justify the application of the exemption under s 33(a)(i). The applicant rejects the respondent's arguments for the application of s 47E(d) for the same reasons he rejects the respondent's arguments for the application of s 33(a)(i) in paragraphs [27]-[61] above.

Application of s 11A(5) – public interest

72. If the respondent satisfies the Tribunal that s 47E(d) applies to conditionally exempt the App source code from disclosure, the applicant contends that the respondent cannot satisfy the Tribunal that disclosure of the App source code would, on balance, be contrary to the public interest under s 11A(5) of the FOI Act.

73. The applicant contends that the factors favouring disclosure of the App source code significantly outweigh the Government's continued ability to maintain the security of its systems through non-disclosure of the App source code.

74. The applicant contends that release of the App source code would inform debate on a matter of public importance (**FOI Act s 11B(3)(b)**; **OAIC Guidelines [6.231(b)]**). The myGov System is used by millions of Australians to engage with government services. The development, operation and security of the myGov System, and its constituent or related components including the App, is a matter of public importance. Access to the source code of the App will inform debate on this matter of public importance by revealing information about how the myGov Code Generator App was developed and how it operates, and by giving Australian citizens confidence that the myGov System is fit for purpose and secure.

75. The applicant contends that release of the source code of the App would promote effective oversight of public expenditure (**FOI Act s 11B(3)(c); Guidelines [6.231(c)]**), because the source code provides insight into how the App was developed and those insights are not ascertainable from the compiled App but only through access to the source code (**FT-A [9]; Teague Report [4]-[10]**). Such insights include:

    1. Have industry best practices been followed in the implementation of the App?

    2. Has the agency implemented functionality where a pre-existing "library" (**Teague report [7]**) or platform feature could have provided the same functionality?

76. Agencies including the DTA (**FT-A [26]**) and the UK Ministry of Justice (**FT-A [53]**) recognise the value of disclosing source code for financial accountability and to reduce costs. Disclosure of the App source code would reveal whether Services Australia has expended resources in an appropriate and efficient manner.

77. The applicant contends that release of the source code of the App would advance the fair treatment of individuals and other entities in accordance with the law in their dealings with agencies (**OAIC Guidelines [6.231](i)**), in two ways:

    77.1. First, the official App was only available from the official Google Play Store. Access to the Play Store requires the user to have a Google user

account, and to log into that account on their mobile device. The effect of this is that access to Australian Government services (or a mechanism to enhance login security) is mediated through a foreign corporation. Disclosure of the source code of the App would allow the legitimate App to be made available through other mechanisms.

77.2. Second, the App was only available for Android devices (via Google Play Store) and Apple iOS devices such as iPhone (through Apple's App Store). These represent a large majority but not the totality of mobile devices. Disclosure of the source code of the App would enable the legitimate App to be adapted for devices and platforms not supported by the official App.

78. The applicant contends that release of the source code of the App would contribute to innovation and the facilitation of research (**OAIC Guidelines [6.231](k)]**), in the following ways:

78.1. Facilitate research on the security of the application, and the security of the myGov system in general. The COVIDSafe experience (**FT-A [36]-[40]**), and the substantial research and reverse engineering work that has been performed regarding the myGov Code Generator App without access to its source code (**FT-A [73]-[86]**), show that these outcomes are likely, not theoretical. The ability to analyse source code leads to improved security outcomes (**Teague Report [49]-[53]; FT-A, FT 13, p 208; FT-A, FT-16, page 222**).

78.2. Facilitate the kind of innovation described above (paragraph [77.2]), that is: adapting the application for use on additional mobile platforms, or creation of compatible alternatives, to allow more people to securely access the myGov system.

78.3. Facilitate innovation and development to improve the usability and accessibility of the application. For example: improving the user experience for people with disabilities; translating or modifying the application to better serve culturally and linguistically diverse users; and general improvements to the user experience, performance or security of the application. The COVIDSafe experience (**FT-A [36]-[40]**) and the experience of the UK Ministry of Justice (**FT-A, FT-16, page 220**) shows that these outcomes are likely, not theoretical.

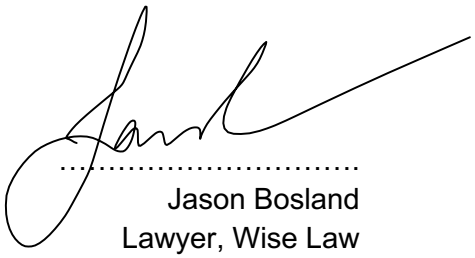
78.4. Facilitate the reuse of the App's implementation, or parts of the implementation, in other digital solutions (**FT-A [26], FT-4, page 39; FT-13, page 206; FT-16, page 220**).

PART IV CONCLUSION

79. The Tribunal should find that the respondent has not established that the App source code is exempt from disclosure under either ss 33(a)(i) or 47E(d) of the FOI Act.

80. The decision under review should be set aside, and the Tribunal should substitute a decision granting the applicant's FOI request.

Date: 31/07/2026



.....

Jason Bosland
Lawyer, Wise Law