Fraser Tweedale
foi+request-7566-b23082df@righttoknow.org.au

October 12, 2021

Freedom of Information Team
Information Access Branch — Legal Services Division
Services Australia

Dear Freedom of Information Team,

Reference: LEX 63435

On 13 September, 2021 you made an access refusal decision on my Freedom of Information request, reference **LEX 63435**, for source code and technical documentation of the *myGov Code Generator* application (**the app**). You identified 12 documents within the scope of my request, including source code, solution brief, use case documentation and API documentation. You decided that all 12 documents were conditionally exempt under section 47E(d) of the FOI Act, and that, for each document, release would be contrary to the public interest.

Under s 54(2) of the Freedom of Information Act 1982, I am applying for an internal review of the decision. Below, I give the reasons why I disagree with the decision and discuss additional factors that may not have been considered.

Applicability of Section 47E(d)

In your reasons for decision you stated:

> The information within the documents, to which the conditional exemption has been applied, includes source codes, API documentation, solution brief and use case documentation. Release of this information could allow for duplication of the app design, lead to an increase in phishing attacks, be reused and processed and ultimately threaten the security of government information systems. I am satisfied release of the information could reasonably be expected to increase the risk of unauthorised access to the agency's computer systems and customer records

This paragraph raises a specific concern of *counterfeiting* (which the basis of the phishing concern). It also raises a non-specific concern of "reuse and processing" of information (*abuse of information*) threatening the security of government information systems. I will address these concerns separately in the following subsections.

Counterfeiting

Even without access to source code or other kinds of technical documentation, it would be straightforward for an experienced mobile application developer to develop a counterfeit of the myGov Code Generator application. It is sufficient to observe the appearance and behaviour of the compiled application, extract or reproduce its media assets (icons, images, animations, sounds, etc), then build a program that is superficially similar in appearance and behaviour.

It should be noted that, from a user's point of view, the myGov Code Generator application is simple. It consists of an enrolment feature, where the user supplies their myGov credentials, and the code generation feature. An experienced mobile app developer could replicate the entire user experience of the app in a short time (perhaps as little as a few hours), without access to source code or technical documentation of the app.

For these reasons, access to the source code or technical documentation is not a prerequisite for creating a malicious application that masquerades as the myGov Code Generator application. Keeping this information non-public is not a substantial barrier to such activity.

After creating a counterfeit application, the problem of distribution remains. That is, how will the counterfeit application actually get installed and run on user devices?

Services Australia distributes the Android myGov Code Generator application exclusively through the Google Play Store. Likewise, you distribute the iOS version of the application for Apple devices exclusively through the Apple App Store. It is useful to consider the general characteristics of this "app store" distribution model.

App stores provide access to curated collections of applications for a particular device or family of devices, and a mechanism of secure distribution of those applications (possibly for a fee, though the myGov Code Generator app is provided without charge). The Apple App Store is managed by Apple, and the Google Play Store is managed by Google.

Overwhelmingly, users of Android devices use the Google Play Store as the primary and default way to find and install applications on their device, and users of Apple devices use the Apple App Store. It is possible for advanced users to install applications from other sources, but it is reasonably expected that such users know how to, and would, authenticate the sources.

These app stores prominently display the publisher of every application. This information comes from verified information about the owner of the account that publishes the application. For example, Google Play Store prominently identifies Services Australia as the publisher of the app. A

counterfeit application would have a different entity prominently identified as its publisher.

Apple App Store and Google Play Store Terms of Service prohibit applications that impersonate other applications. The app store applications have features to report problematic applications, such as counterfeits. Apple and Google also allows developers to submit removal requests for applications that violate the Terms of Service, infringe on trademarks or copyright, or violate other laws. The operators take proactive steps to detect and remove counterfeit applications from their app stores.

To summarise my arguments in this section:

- Source code and technical documentation are not prerequisites to developing a counterfeit application.
- The "app store" distribution model provides significant safeguards and recourse against counterfeit applications. These safeguards are at work, and recourse against counterfeit applications may have to be taken, whether or not the myGov Code Generator source code or technical documentation is available to the public.
- End users will overwhelmingly download the myGov Code Generator application from app stores. It is reasonable to expect that users who install it from other sources are advanced users who would take steps to authenticate the application bundle before installing and using it.

For these reasons, I argue that with respect to the counterfeiting concern, releasing the source code of the myGov Code Generator application would not prejudice or have a substantial adverse impact on Services Australia's operations.

Abuse of information

Having addressed the counterfeiting concern in the preceding subsection, in this section I address the more general concern of abuse of information.

The reasons for decision state:

> this information could... be reused and processed and ultimately threaten the security of government information systems.
>
> ...
>
> Disclosing the documents to the world at large under the FOI process could reasonably be expected to... result in this information being used by nefarious actors to circumvent security features and allow access to personal information of third parties. This in turn would have a substantial adverse effect on the

> proper and efficient conduct of the operations of the agency...

The section 93A FOI Guidelines (*Guidelines*) paragraph 6.101 states:

> 6.101 For the grounds in ss 47E(a)–(d) to apply, the predicted effect needs to be reasonably expected to occur. The term 'could reasonably be expected' is explained in greater detail in Part 5. There must be more than merely an assumption or allegation that damage may occur if the document were to be released.

I am a software engineer and have worked on identity management, authentication and public key infrastructure systems for the last 7 years. From a security perspective, there does not seem to be anything novel about the myGov Code Generator application. It consists of an enrolment phase (which handles the user's myGov credentials) and the code generation phase, which appears to use an ordinary OTP (*one-time password*) algorithm. I assume that the architects and developers of the app have taken due care in its design and implementation, and that Service Australia has performed or procured security audits of the program. If these assumptions hold, then it is not reasonable to expect that the release of the source code or other technical information would have a substantial adverse effect.

Access to source code and technical documentation (such as API documentation) is not a prerequisite for finding potential vulnerabilities in a software system. Many vulnerabilities are discovered without any access to such information. For example, security researchers who had no access to source code or technical documentation have discovered and disclosed weaknesses in the ATO's myGovID system and applications[1]. Furthermore, access to source code and technical documentation invites research and analysis, enabling the responsible disclosure of vulnerabilities and counterbalancing the risk posed by nefarious actors (a risk that exists with or without access to the documents that are the subject of this request).

For these reasons, with respect to abuse of the information, release of the source code and technical documentation about the myGov Code Generator app could not reasonably be expected to have a substantial adverse effect on the operations of Services Australia.

Finally, *Guidelines* states:

> **Reasons behind predicted effect**
>
> 6.103 An agency cannot merely assert that an effect would occur following disclosure. The particulars of the predicted effect should be identified during the decision making process, including whether the effect could reasonably be expected to occur.

[1] https://thinkingcybersecurity.com/DigitalID/

> Where the conditional exemption is relied upon, the relevant particulars and reasons should form part of the decision maker's statement of reasons, if they can be included without disclosing exempt material (s 26, see Part 3).

I do not believe that the reasons given, with respect to the *abuse of information* concern, are specific enough to rely upon the s 47E(d) conditional exemption. The particulars that give rise to a reasonable expectation of adverse effect were not described in sufficient detail.

Furthermore, the fact of the expected effect and whether it could be reasonably expected to occur must be established separately for each of the 12 documents identified. The schedule of documents describes several different kinds of documents: source code, solution brief, use case documentation and API documentation. These kinds of documents contain different kinds of information. Therefore the particulars of the predicted adverse effect, the information that gives rise to it, and the reasons why it would be reasonably expected to occur, are likely to differ between the identified documents.

Public interest factors

If any of the documents are found to be conditionally exempt under s 47E(d), then it is necessary to weigh the public interest factors favouring and against disclosure and determine whether access is contrary to the public interest. Non-exhaustive lists of factors favouring and against disclosure are given in *Guidelines* s 6.19 and s 6.22, respectively.

Your decision stated:

> When weighing up the public interest for and against disclosure under section 11A(5) of the FOI Act, I have taken into account relevant factors in favour of disclosure. In particular, I have considered the extent to which disclosure would promote the objects of the FOI Act.
>
> I have also considered the relevant factors indicating access would be contrary to the public interest. In particular, I have considered the extent to which disclosure could reasonably be expected to:
>
> - increase the likelihood that the information will be used by nefarious actors, to circumvent security features
> - increase the risk that the myGov Code Generator app could be duplicated, leading to a phishing attack on the agency or individuals.

- prejudice the agency's ability to properly and efficiently deliver services to the public
- prejudice the agency's ability to meet its obligations under the Privacy Act 1988 (Cth) (specifically, Australian Privacy Principal 11)
- prejudice the myGov Code Generator app's integrity, and
- prejudice the security of the agency's computer systems.

The only factor favouring release that seems to have been considered was 6.19(a), *promotes the objects of the FOI act*. The stated factors against release were considered to outweigh the factor in favour. However, the release of the myGov Code Generator source code and technical documentation engages several public interest factors favouring disclosure that were not weighed in the original decision. I discuss the factors against and favouring disclosure in sections that follow.

Factors against disclosure

increase the likelihood that the information will be used by nefarious actors, to circumvent security features

As discussed in previous sections, I believe there is a low risk of nefarious actors discovering serious vulnerabilities *that would not otherwise be discoverable* without the release of the documents. Furthermore, if there are security vulnerabilities in the myGov system, release of source code and technical documentation enables security researchers to discover and responsibly disclose them so they can be fixed.

increase the risk that the myGov Code Generator app could be duplicated, leading to a phishing attack on the agency or individuals.

As discussed in previous sections, the risk of counterfeit applications exists regardless of the availability of source code or technical documentation. Unavailability of such information is not a significant impediment to the development of a counterfeit app. The app store distribution model, which would remain the primary distribution model even after disclosure of these documents, provides some protection and recourse against this risk.

prejudice the agency's ability to properly and efficiently deliver services to the public

prejudice the agency's ability to meet its obligations under the Privacy Act 1988 (Cth)

prejudice the myGov Code Generator app's integrity

prejudice the security of the agency's computer systems.

It is unclear how these four factors arise, other than as consequences of the factors already discussed (*abuse of information* and *counterfeiting*) rather than as substantive factors in their own right.

Factors favouring disclosure

6.19(a) promotes the objects of the FOI Act

The original decision agrees that the release of the source code would promote the objects of the FOI Act, though it does not go into further detail. Two objects of particular relevance to this request are 3(2)(a):

> increasing public participation in Government processes...

and 3(3):

> ...increase recognition that information held by the Government is to be managed for public purposes, and is a national resource.

6.19(b) inform debate on a matter of public importance

The myGov system is used by many citizens and residents of Australia to engage with a variety of essential government services. Therefore transparency about the development, operation and security of the myGov system, and its constituent or related components including the myGov Code Generator application, is a matter of public importance. Availability of the source code and technical documentation of the app will enhance public awareness and understanding and inform debate on this matter of public importance.

6.19(c) promote effective oversight of public expenditure

Significant and ongoing public expenture enables the development, maintenance and operation of the myGov system, including the myGov Code Generator app. Release of source code and technical documentation promotes oversight of this expenditure.

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

I am not aware of any law concerning the means of access to government services and restriction of access to particular technological devices (hardware or software). I therefore discuss this matter in the *spirit* of public interest factor 6.19(i), that is, *fair treatment of individuals*, and note that the list of public interest factors in *Guidelines* is non-exhaustive.

Services Australia publishes the myGov Code Generator apps for the Android and Apple iOS operating systems, which are used on mobile phones

and other portable computers. Android and Apple iOS devices are popular and together constitute a large portion of the market. However, some people do have other kinds of mobile devices, and I am one such person. Neither version of the myGov Code Generator app published by Services Australia is compatible with my device.

Furthermore, even for users of Android or Apple iOS devices, one can only access the myGov Code Generator app via the Google Play Store (for Android) or Apple App Store (for iOS). This requires registering an account and providing personal details to Apple or Google. These are foreign companies who act in the interests of their shareholders, not account holders.

I accept that Services Australia cannot and should not attempt to create and distribute a version of the app for every device or operating system in the market. I also accept that it is reasonable to use the Google Play Store and Apple App Store as the primary distribution channels for the Android and iOS versions of the app, respectively. But consideration should be given to the individuals who do use other kinds of devices or who do not wish to become Google or Apple account holders and run proprietary, opaque software on their device in order to access Australian government services.

Releasing the source code and technical documentation of the myGov Code Generator app would advance the fair treatment of individuals by Services Australia (and by other agencies who operate services that can be accessed via myGov) in two significant ways.

First, the program can be adapted to other platforms. Or, with the understanding afforded by access to the source code and/or other technical documentation, compatible programs can be written for other platforms. This involves skill, but it need only be done once for each platform, and the resulting artifact can be distributed to many users (including those without the necessary skills to "port" the program themselves). As a result, more people will be able to access the myGov system and the services offered through it.

Second, users of Android or iOS devices will be able to access the myGov Code Generator application without needing to register an account with Google or Apple.

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

Access to the source code of the myGov Code Generator application will facilitate research on the security of the application, and the myGov system in general.

Access to the source code will also facilitate the kind of innovation described

in the preceding subsection, that is: porting the application to additional mobile platforms, and/or creation of compatible programs, to allow more people to access government services via myGov.

Access to the source code facilitates innovation and development to improve the usability and accessibility of the application. For example:

- Improving the user experience for people with vision impairments or impairments that affect or prevent physical interaction with a mobile device.
- Translating or otherwise modifying the application to meet the needs of culturally and linguistically diverse cohorts of users.
- General improvements to the user experience, performance or security of the application.

If Services Australia is so disposed, they can make it possible to incorporate improvements developed in the community back into the myGov Code Generator application. This kind of software innovation can be collaborative rather than independent or adversarial.

Compliance with Digital Service Standard criterion 8

The Australian Government Digital Transformation Agency (DTA) publishes the *Digital Service Standard*, which it defines as

> a set of best-practice principles for designing and delivering government services. It helps digital teams to build services that are simple, clear and fast.

The DTA provides a description[2] of which services are covered by the standard, which states:

> The Digital Service Standard applies to Australian Government services that are:
>
> - public facing
> - owned by non-corporate Commonwealth entities
> - new informational or transactional services (designed or redesigned after 6 May 2016)
> - existing high-volume transactional services
>
> ...

[2] https://www.dta.gov.au/help-and-advice/digital-service-standard/services-covered-standard

> Information services are typically websites or mobile applications that provide information to the public. This information includes reports, fact sheets and video.
>
> ...
>
> Transactional services are any services that lead to a change in the records held by government.
>
> ...
>
> **High-volume transactional services**
>
> These are services that process (or are likely to process) more than 50,000 transactions every year.

The myGov service, and in particular the myGov Code Generator app, are covered by the standard.

Criterion 8 of the standard is *Make source code open*[3]. The standard discusses why it is important and what the benefits are.

This criterion is discussed further in a post[4] on the DTA blog. In particular, it elaborates that security concerns are rarely a valid reason to keep source code secret, and that there is a public interest in sharing the source code:

> Government code should be available to others unless there is a compelling reason. Everyone in the public service benefits from being able to reuse code that others have developed. We all work for the taxpayer and they should be able to see and use what theyve paid for.
>
> ...
>
> Once teams understand more about what open source is, and isnt, they find they dont usually have any reason not to be open. However, it is common for teams to be concerned about security.
>
> Security is a very valid reason, but you shouldn't use it as an excuse to close everything. Keeping passwords and keys private helps to keep our users data private and secure. Not only is it good practice, its part of the obligation we have in serving the public. Code that doesn't contain these secrets can be shared and reused by others.

[3] https://www.dta.gov.au/help-and-advice/digital-service-standard/digital-service-standard-criteria/8-make-source-code-open

[4] https://www.dta.gov.au/blogs/making-source-code-open

Closing

Thank you for considering my submissions and I look forward to the completion of the review.

Sincerely,

Fraser Tweedale